



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2009-03

Feasibility study of network operations center collaboration to improve application layer performance

Meyer, Kent A.

Monterey, California: Naval Postgraduate School

<http://hdl.handle.net/10945/4805>

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**FEASIBILITY STUDY OF NETWORK OPERATIONS
CENTER COLLABORATION TO IMPROVE APPLICATION
LAYER PERFORMANCE**

by

Kent Meyer

March 2009

Thesis Advisor:

Alex Bordetsky

Second Reader:

Karl Pfeiffer

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Feasibility Study of Network Operations Center Collaboration to Improve Application Layer Performance			5. FUNDING NUMBERS	
6. AUTHOR(S) Meyer, Kent A.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) Network Centric Warfare seeks to improve the link between the shooter and sensor networks, enabling direct access to pertinent information and a shorter decision loop with improved operational capabilities. The sensor-shooter network is often conceptualized in two network models: centralized and decentralized. Centralized networks can provide robust management of network resources but potentially lengthens the decision process while information is routed through distant nodes or becomes delayed in lengthy queues. Comparably, decentralized networks can potentially speed up the decision process by direct access to information. Decentralized networking does not promote efficient management of network resources since all users are able talk to each other and overload the network. To overcome the high utilization of resources network operations centers (NOCs) on decentralized networks can manage resources by collaborating with other NOCs. A NOC can be any device that monitors, reports and manages resources. NOC-to-NOC collaboration would allow for greater efficiency using network resources by allowing for prioritization and protection of critical services determined by the operational user. To allow effective collaboration and management we must define what information needs to be monitored and how to manage this information. The information set and usage will be defined in this thesis.				
14. SUBJECT TERMS Network Operations Centers, Collaboration, Task Force ODIN, peer-to-peer, Network Centric Warfare, Network Management, Application Layer Performance			15. NUMBER OF PAGES 111	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std.

Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

**FEASIBILITY STUDY OF NETWORK OPERATIONS CENTER
COLLABORATION TO IMPROVE APPLICATION LAYER PERFORMANCE**

Kent A. Meyer
Lieutenant Commander, United States Navy
B.S., North Carolina State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
March 2009**

Author: Kent Meyer

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Lt. Col. Karl Pfeiffer, USAF
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network Centric Warfare seeks to improve the link between the shooter and sensor networks, enabling direct access to pertinent information and a shorter decision loop with improved operational capabilities. The sensor-shooter network is often conceptualized in two network models: centralized and decentralized. Centralized networks can provide robust management of network resources but potentially lengthens the decision process while information is routed through distant nodes or becomes delayed in lengthy queues. Comparably, decentralized networks can potentially speed up the decision process by direct access to information. Decentralized networking does not promote efficient management of network resources since all users are able to talk to each other and overload the network. To overcome the high utilization of resources network operations centers (NOCs) on decentralized networks can manage resources by collaborating with other NOCs. A NOC can be any device that monitors, reports and manages resources. NOC-to-NOC collaboration would allow for greater efficiency using network resources by allowing for prioritization and protection of critical services determined by the operational user. To allow effective collaboration and management we must define what information needs to be monitored and how to manage this information. The information set and usage will be defined in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	OVERVIEW	1
B.	NETWORK CENTRIC WARFARE IMPROVEMENT OF THE SENSOR-SHOOTER NETWORK	2
C.	CURRENT STATE OF SENSOR-SHOOTER NETWORK MANAGEMENT ...	5
D.	FUTURE NETWORK MANAGEMENT POSSIBILITIES	7
II.	LITERATURE REVIEW	9
A.	OVERVIEW	9
B.	NETWORK MODELS	9
1.	Centralized Networks	9
2.	Decentralized Networks	11
a.	<i>Ad-hoc Networks</i>	11
b.	<i>Hybrid Peer-to-Peer Networks</i>	11
C.	NETWORK MANAGEMENT	13
D.	COLLABORATION	15
1.	Definition	15
2.	Methods	16
3.	Benefits	17
4.	Challenges	17
E.	TASK FORCE ODIN (TF ODIN): REAL-WORLD EXAMPLE OF A SENSOR-SHOOTER NETWORK USING COLLABORATION	19
1.	Background	19
2.	Network Structure	19
3.	Operations	21
4.	Applying the TF ODIN Model to Operations and USSOCOM Expert Networks	22
III.	NETWORK MANAGEMENT AND COLLABORATION METHODOLOGIES	25
A.	OVERVIEW	25
B.	NETWORK MANAGEMENT APPROACHES FOR APPLICATION PERFORMANCE	25
1.	ICMP and SNMP	25
a.	<i>Internet Control Messaging Protocol (ICMP)</i>	25
b.	<i>Simple Network Management Protocol (SNMP)</i> ..	26
2.	Active SNMP and Network Modeling	28
3.	Network Aware Nodes/8th Layer Concept	29
4.	NetFlow, sFlow, IPFIX	30
a.	<i>NetFlow</i>	30
b.	<i>sFlow</i>	32
c.	<i>IP Flow Information Export (IPFIX) Protocol</i>	33
5.	Quality of Service by Bandwidth Allocation	33
a.	<i>Bandwidth Allocation Auctioneering Mechanism</i>	33

b.	<i>Information Management Brokers for Cursor on Target (CoT) Messaging.....</i>	36
c.	<i>Situation Aware Protocols in Edge Network Technologies (SAPIENT) Program/Synthesizing Adaptive Protocols by Selective Enumeration (SYNAPSE).....</i>	37
C.	COLLABORATION METHODOLOGIES	38
IV.	EXPERIMENTATION AND RESULTS	41
A.	TNT NETWORK TOPOLOGY	41
1.	TNT Experiment Testbed.....	41
2.	TNT OFDM Backbone.....	41
B.	EXPERIMENT SCENARIOS	43
1.	Battle Field Medical Scenario.....	43
2.	ODIN Counter-IED Scenario.....	46
C.	EXPERIMENT MEASURES	49
1.	Collaboration Measures.....	49
2.	Application Monitoring Using SFlow.....	50
3.	Usability of Network Applications.....	51
D.	EXPERIMENT RESULTS	52
1.	Battlefield Medical Results.....	52
2.	ODIN Counter-IED Results.....	56
3.	Overall TNT 09-2 Experiment Results.....	58
a.	<i>Parafoil Drop and Control Experiment.....</i>	58
b.	<i>Network Monitoring of Redline AN-80i Radio.....</i>	59
V.	CONCLUSIONS AND FUTURE WORK	63
A.	CONCLUSIONS	63
1.	NOC-to-NOC Collaboration	63
2.	Application Monitoring and Performance.....	65
3.	Meeting the Commander's Intent by Maintain Situational Awareness.....	66
B.	FUTURE WORK	67
APPENDIX A:	CHAT DATA CAPTURES	69
A.	BATTLEFIELD MEDICAL CHAT DATA	69
B.	TF ODIN CHAT RESULTS	73
C.	TF ODIN OBSERVERS NOTE PAD DATA	77
D.	PARAFOIL SIGNIFICANT EVENTS RECORD	80
E.	REMOTE MONITORING OF REDLINE RADIO AN-80I CHAT LOG ..	82
APPENDIX B:	SFLOW SCREEN CAPTURES	83
LIST OF REFERENCES	89
INITIAL DISTRIBUTION LIST	95

LIST OF FIGURES

Figure 1.	Variation of Quality of Service Across the Warfighting Enterprise (From [5, 6]).....	4
Figure 2.	Network Centric Warfare Framework (From [7]).....	4
Figure 3.	Summary of NCW Framework Attributes (From [7])...	5
Figure 4.	Client-Server Network Model.....	10
Figure 5.	Ad-hoc Network Model.....	12
Figure 6.	Conceptual Network Model for TF ODIN (From[17])..	21
Figure 7.	One-to-Many SNMP Organizational Model (From [22]).....	27
Figure 8.	NetFlow Datagram.....	31
Figure 9.	Deployed CoT Messaging Network (From [30]).....	35
Figure 10.	Basic CoT Message Flow (From [30]).....	36
Figure 11.	SYANPSE Protocol Framework (From [34]).....	38
Figure 12.	TNT Network Diagram (From [35]).....	42
Figure 13.	Battle Field Medical Scenario Network Topology..	44
Figure 14.	Battlefield Medical Collaboration Network.....	45
Figure 15.	ODIN Counter-IED Scenario Network Topology.....	47
Figure 16.	ODIN Counter-IED Collaboration Network.....	48
Figure 17.	sFlow Agent-Collector Configuration.....	51
Figure 18.	Video Conference for Battlefield Medic in VC1...	52
Figure 19.	Network Status for Battlefield Medic.....	54
Figure 20.	NPS sFlow Network Load for Battlefield Medic....	55
Figure 21.	NPS sFlow Bandwidth Usage for Battlefield Medic..	55
Figure 22.	ODIN Mobile Network Status, Loss of Link.....	58
Figure 23.	Redline AN-80i Network Discovery.....	60
Figure 24.	Redline AN-80i Initial Performance Monitoring...	61

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Functional Areas of Network Management.....	14
Table 2.	Military Benefits of Collaboration applied to Network Operations.....	18
Table 3.	Barriers to Collaboration in the Military.....	18
Table 4.	32 bit sFlow Datagram (From [26]).....	32
Table 5.	Additional sFlow Monitoring Parameters over NetFlow (From [27]).....	32
Table 6.	Collaboration Methodologies Matrix.....	39
Table 7.	Battlefield Medical Collaboration Matrix.....	46
Table 8.	ODIN Counter-IED Collaboration Matrix.....	49

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to first and foremost thank my family, without whom I do not believe I could have had the drive and motivation to undertake this task. I would like to express my deepest thanks to them for allowing me time away to complete my studies.

Thanks are in order for Dr Alex Bordetsky who allowed me a vast amount of freedom to explore this topic and gave me encouragement and guidance in expressing my ideas. Thank you to Mike Clement and Buddy Barreto who listened to some off-the-wall ideas during my exploration process. Thank you to Eugene Bourakov who is a technical master that created many programs used in this research. Thanks are also owed to Lieutenant Colonel Karl Pfeiffer for working with a former engineer on correct prose and grammar and for helping me express my ideas on paper.

Finally, thank you to all the friends I have made at the Naval Postgraduate School. You have increased the enjoyment of the Monterey Tour.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Basic military operations that involve the possibility of conflict require the operator to identify their target before engaging. Engagement of that target requires positive identification including operational constraints (i.e., non-combatants, location, weapons restrictions, covertness, enemy capabilities, etc.). This list is not all-inclusive, but it allows the military operator, or shooter, to determine tactical courses of action to neutralize the threat or accomplish mission objectives. Historically, a shooter remotely observing a target used a scout to act as a sensor. The scout would observe the target and then report their findings back to the shooter so they could make a decision on how to engage. The scout was limited in their means to observe and communicate their findings. Observation was limited by their senses and the communication of their findings was limited by speech and time-delayed photography, which were transmitted either in person or by radio.

Modern military operations apply technologies that enable the shooter to detect and observe their target at a much greater distance and with much greater detail compared to human senses. Sensors now have the ability to detect the electromagnetic spectrum, non-visible light, and slight variations in objects over time. Modern sensor platforms now have the ability to transmit their data and provide streaming video in near real-time to the shooter and operate in extreme conditions while being controlled

remotely. For this discussion the sensor, the object that detects and the sensor platform, the object the transports the sensor, will be commonly referred to as the sensor. An example of a modern sensor is the Unmanned Aerial Vehicle (UAV) that can provide streaming video and Intelligence, Surveillance and Reconnaissance (ISR) capabilities to a commander that is located hundreds of miles away. Not only has the sensor advanced in its capabilities but the communications link that provides the shooter with their information has advanced thanks to internet based technologies and advance wireless communications.

The increase in sensor capability has resulted in more data transmitted to aid the shooter in the decision making process. The increase in data has required the network to expand in capacity and complexity so it can deliver this glut of data. The complex network that delivers the data now needs to be managed so that it is available, reliable and secure. It is also common that the data a sensor sends to the shooter travels over multiple networks before it reaches the shooter. To ensure the shooter has access to the sensor data and to ensure that the sensor can transmit the network must be managed to provide an adequate quality of service. The more complex the network becomes the harder the management becomes. It is also important to note that the management of the network has the greatest impact on the quality of service that it delivers [1].

B. NETWORK CENTRIC WARFARE IMPROVEMENT OF THE SENSOR-SHOOTER NETWORK

Network Centric Warfare (NCW) has the ultimate goal of providing information superiority to the warfighter

resulting is the successful completion of the commander's intent [2]. In the context of military operations, information superiority is currently defined as:

Information superiority is described as the operational advantage gained by the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. [3]

For the sensor-shooter network, NCW aims to improve way sensors and shooters are linked together and how they share information. The third concept of NCW, effective linking, describes how the improvement of the sensor - shooter link will facilitate adaptability, synergy, and increased combat power. Access to high quality information and self-synchronization requires a highly capable and highly robust network [4]. The high performance network is the backbone that enables the shooter to get the right data at the right time. The requirement for data timeliness and precision as it applies to the scale of military operations is illustrated in Figure 1.

NCW is not about the network that the data travels on, but it is contingent on having network capable of providing a minimum level of quality of service for NCW effect to occur. This network infostructure is referred to as the 'Entry Fee' [6]. The framework of NCW indicates that the Degree of Networking is an entry point into the NCW process as seen in Figure 2.

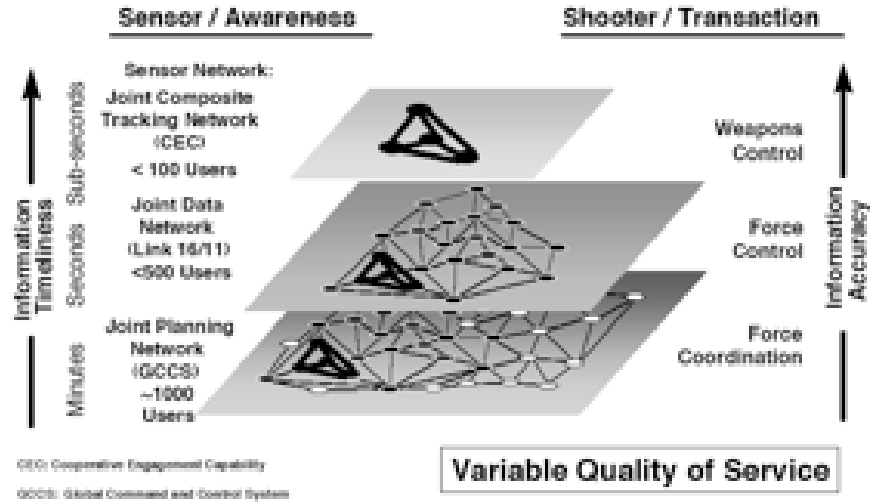


Figure 1. Variation of Quality of Service Across the Warfighting Enterprise (From [5, 6])

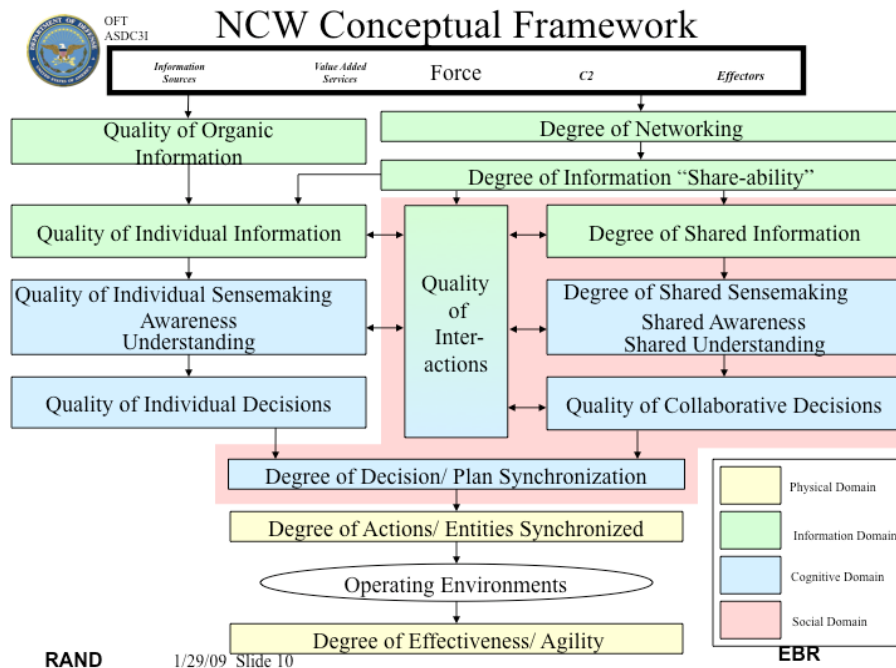


Figure 2. Network Centric Warfare Framework (From [7])

The Degree of Networking is determined by the quality attributes of the network [7]. The quality attributes can be broken out as seen in Figure 3. Many of the networking attributes describe the performance characteristic of the network. Maintaining high network performance is a desirable goal for Network Operations Centers (NOCs). The entry point into the NCW framework is where the role of the NOC is critical in providing the foundation of a highly robust and highly capable network. The more complex the network becomes the more important the role of the NOC becomes.

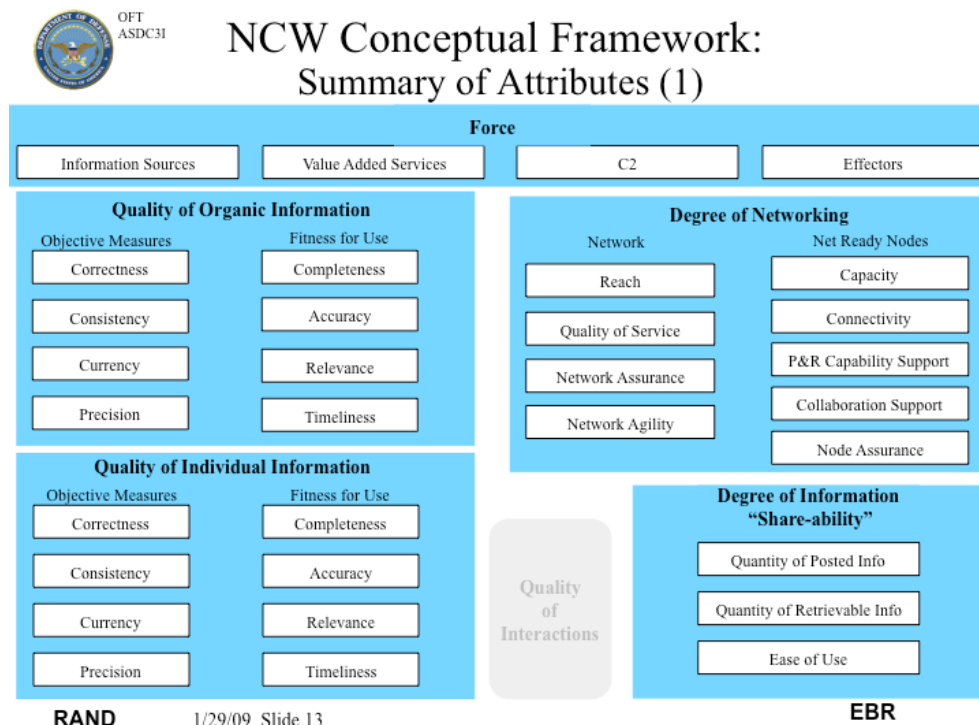


Figure 3. Summary of NCW Framework Attributes (From [7])

C. CURRENT STATE OF SENSOR-SHOOTER NETWORK MANAGEMENT

The sensor-shooter network is an evolving and dynamic network that provides information in various environments

throughout the world. The modern sensor-shooter network is also adopting the use of Internet technologies to form the network and distribute information used by the warfighter. Internet Protocol (IP) is common protocol for NCW, data exchange and the Global Information Grid (GIG) [8]. The use of legacy sensor technologies and communications equipment on the GIG (i.e., military radios, satellites, etc.) restricts how sensor-shooter networks are linked, designed and operated. Legacy equipment needs to have a translator to move data from one network to the next because they may use a specialized communication protocols or data formats not readable by another source. The translator can be a person typing information from one network on to another or a piece of technology that performs the translation. It is important to note that the translator bridges two or more distinct networks that will need to be managed separately. The holistic sensor-shooter network is typically made up of multiple networks that are geographically dispersed. The sensor has a way of communicating its data to a central source and the shooter typically will use a different network of receiving data they need and communicating back to the command center. This is in part due to the stovepipe design and procurement processes that developed the infrastructure for the shooter and sensor. The result is that there are multiple networks that all need to be managed individually to ensure that each component has the best network to perform their mission. The management of these networks is typically isolated from other NOCs and the local NOC is concerned with optimizing their network and ensuring their communications interfaces are operational. In some cases,

the NOC may be aware of the specific mission that they are supporting. This network management practice can result in sub-optimization of the entire sensor-shooter network, which ultimately limits the maximum effectiveness of the NCW framework.

D. FUTURE NETWORK MANAGEMENT POSSIBILITIES

To provide a high quality of service network that NCW requires the most important action that can be taken is effective management of the network. The current state of network management systems does not provide adequate level of performance alone to achieve this high level of network performance [1]. Using a principle of NCW, self-synchronization, NOCs can attempt to better manage their networks and provide a better overall service to the commander, operator, sensor and shooter. NOC-to-NOC collaboration will allow NOCs to share information on network performance, application priority and mission goals so they can better work together to ensure the critical services are identified and protect those services necessary for completing the commander's intent. In this case, services will be any application that is need by the shooter to be successful (i.e., streaming video, chat, imagery, email, voice, etc.).

The challenge of NOC-to-NOC collaboration is defining a common set of parameters to monitor, monitoring them and gathering the information from the data collected and sharing it. The sharing of information will increase the collective knowledge of the NOCs working together. This will enable greater effective management of the entire sensor-shooter network instead of the sub-optimized

alternative. NOCs will need to be loosely connected to share their information and they will need to have a common set of parameters to monitor including the commander's priorities. The NOC-to-NOC collaboration will also involve the operational decision maker who will provide input on desired network services.

II. LITERATURE REVIEW

A. OVERVIEW

The goal of this research is to define an initial set up parameters that can be measured, monitored and shared by a NOC to be used in NOC-to-NOC collaborations. The initial set of parameters is not meant to be inclusive and will not be entirely contained within the network. The parameters will also include external information such as Commander's Intent, critical applications and other rapidly changing user-defined parameters that are not represented in the network traffic. This chapter is dedicated to review current networks and their management practices including future capabilities. The focus of network management will be on providing the best service to the user. In this case, NOCs will be conducting at application management as the primary focus versus link or network performance. This chapter will also define and contextualize terminology and give examples of a real world networks that will be modeled for experimentation. The academic foundation will be placed in the areas of network management and collaboration.

B. NETWORK MODELS

1. Centralized Networks

In centralized networks, all data and requests for data flow through a single point of control. A common application of centralized networks is the client server model. In this model, a client will request data or a service from a server. The server will then authenticate

the user's request and determine if it has the data or service available. If the request is available, the data is returned. If it is not available, the request may be forwarded on to another server, or a reply is sent that the request was not found. It is important to note that in Client-Server networks, the client does not share any information or resources with the rest of the network. The Server is responsible for providing the high-power resources and information to the client requests [9].

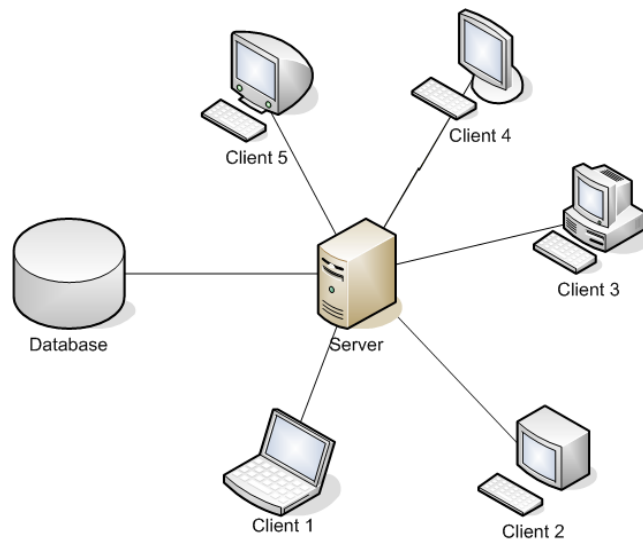


Figure 4. Client-Server Network Model

The benefits of client-server networks is that it is an easier network to manage, easier to scale in both hardware and function since the server hosts all the resources, and it has the least amount of network traffic overhead as the server also manages the traffic flow of requests. The downsides to client-server networks is the upfront cost required to buy specialized equipment, the specialized training required to administer the server and

– if there are any problems with the server – information or network functionality can be lost.

2. Decentralized Networks

Peer-to-Peer (P2P) networks are a group of computers that share their resources (applications, processing power, storage, etc.) with the other participants in the network without the use of an intermediary agent [9]. A peer in the P2P network acts both as a Client and a Server. In decentralized networks, peers can talk to each other directly without having to go through a central server. A peer that requests information (client) or the use of an application can directly get that information/resource by directly communicating to the peer that has that has the request (server). Two examples of peer-to-peer networks in operation are the Ad-hoc network and the Hybrid peer-to-peer network.

a. Ad-hoc Networks

Ad-hoc networks can be referred to as "Pure" P2P networks because they do not have a central entity in their network [9]. Figure 5 shows an example of an Ad-hoc or "Pure" P2P network. Ad-hoc networks are typically seen used in wireless networks.

b. Hybrid Peer-to-Peer Networks

Hybrid P2P networks have a central entity on their network that act as a directory node to improve the routing of resource requests. The directory node, also called a "hub," "ultrapeer," or "supernode," contains a centralized directory of all the peers, which may be used

by the requesting peer to quickly find the address of requested service instead of broadcasting to all peers on the network [10]. The use of the hub reduces the amount of traffic on the network and can more quickly return the address route. Modern sensor-shooter networks can be modeled as hybrid P2P networks since the sensor is providing data to multiple peers on a network usually through a centralized node, such as a command center.

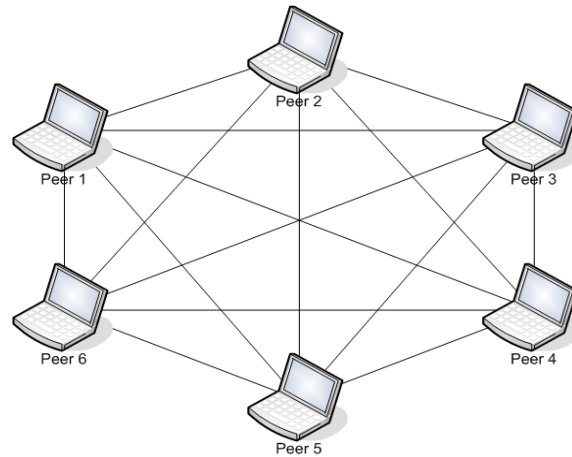


Figure 5. Ad-hoc Network Model

The benefits of peer-to-peer networks are the low cost of equipment purchase since no specialized server is required, P2P networks can take advantage of unused resources on the network, they can be more resilient to failure and traffic flow bottle necks, and they are flexible in their design and implementation. The disadvantages of P2P networks are the limit of their scalability due to the amount of overhead traffic produced, limited in their data throughput due to physical transmission medium and the network overhead, low security, and network maintenance is handled by the user of the specific machine.

C. NETWORK MANAGEMENT

Network management is a broad area that covers more than just the daily operation and maintenance of a computer network. Network management begins with the conceptual design and procurement through operations to include future changes of the network. According to the ISO, there are five functional areas of network management listed in Table 1 [11]. Lundy Lewis describes network management as:

Network management is the practice of (a) monitoring and controlling an existing network so that the network stays up and running and meets the expectations of network users, (b) planning for network extensions and modifications in order to meet increasing demands on network operations, and (c) gracefully incorporating new elements into a network without interfering with existing operations. [12]

An expanded view of network management presented by Subramanian is that network management consists of three areas: Network provisioning, Network Operations, and Network Maintenance. Network provisioning, named the Engineering Group, oversees planning and design and functionally works with network maintenance. The Network Maintenance group also called the Installation and Maintenance (I&M) Group, oversees trouble calls, routine maintenance and testing, installation, and network repair. I&M functionally works with the Engineering Group to install their designs and with the NOC on faults and trouble ticket issues. The last area, Network Operations, named the Operations Group or the NOC, oversees the five areas covered by the ISO [13]. The NOC uses a network management system (NMS) to monitor and operate the network. The NMS takes information from the network and its

components to determine the health of the network. The protocols that are typically used with an NMS are simple network management protocol (SNMP) and common management information service protocol (CMIP). SNMP and CMIP were developed from the OSI network model.

Fault Management	Fault management encompasses the detection, isolation, reporting, correction and recording of errors on the network. Fault detection includes tools to identify root causes of problems, verification of fault correction and trend analysis.
Accounting Management	Accounting management encompasses billing, procurement costs, and operational costs. In the modern business this are could expand to include the value added from information technology and the portfolio management of network assets.
Configuration Management	Configuration management encompasses discovering the network, detecting and implementing changes, controlling the change processes, and maintaining the network inventory.
Performance Management	Performance management encompasses the network performance metrics (i.e., bandwidth, latency, up-time, utilization), network health, application performance and operation of the network under alternate configuration for management activities.
Security Management	Security management encompasses protection of data, authorization of users, maintenance of encryption devices and keys, network usage policies, logging of unauthorized/authorized access and activities, and detection and prevention of viruses and other malicious software.

Table 1. Functional Areas of Network Management

Military operations that involve unconventional missions (including humanitarian/disaster relief, counterterrorism and counter-IED operation) operate using networks that rapidly change, have bandwidth restrictions and are in hostile environments. Given the nature of military operations and military networks, only the higher command structures have robust high capacity networks. Focusing on the tactical user, including the shooter, the body of this thesis will focus on performance management and meeting the user's expectations. The measurement of success for a NOC in the military is that his users have functioning services on the network allowing the commander's intent to be achieved.

Tactical networks, especially sensor-shooter, networks are not composed of one homogeneous type of networks. They typically have multiple specialized networks that are owned and operated by different personnel. The sensor-shooter network can be viewed as a network of networks.

D. COLLABORATION

1. Definition

For the context of this research, collaboration will be used to mean the act of two or more entities that are cooperatively working together to create something greater than the capabilities of a single entity. This definition of collaboration is similar to synergy, but it is used to create an understanding of what collaboration should mean when it is applied to technologies or processes. Traditional definitions of collaboration do not specify whether an entity is a willing participant in the process or if the desire process is designed to produce something

with added benefit. Synergy is melded into this use of collaboration due to its importance in NCW and the desire to have collaborative technologies improve the organization.

2. Methods

The primary focus of collaboration in the context of this thesis will be using Information Technology (IT) collaboration systems and methods to provide a learning environment for Network Operations Centers. Effective collaboration will allow the learning environment to increase knowledge transfer between NOCs and individuals and to create a learning organization as a whole. Learning organizations are ones that continue to enhance their capacity to create [14]. To promote the capacity to create and learn knowledge must be passed from one individual or group to another.

There are various methods, tools and functions of collaboration. Collaboration can take place in person, across vast distance, in real time or asynchronously. There is a wealth of research in the area of collaboration describing the models, tools to be used and how to make it more effective. There is no common model for collaboration, but there are categories that stand out that effect the collaborative process. The areas are distance of separation (in person or remote), medium for communication (telephone, videoconference, email, white board, instant messengers, file sharing, etc.), trust of the organization (personal/peer relationships and freedom from retribution), and trust in the technology (reliable network, ease of use, and functionality). This list is

just a summary of generalized categories that have surfaced while researching collaboration. This research will not attempt to analyze effective collaboration methodologies, but will instead attempt to determine if the right information is identified that will enable effective knowledge transfer, thus enabling the organization to learn and completion of the commander's intent.

Further scoping the problem, this research will focus on remote organizations using electronic communications. The tools used are instant messaging, voice (cellular, landline, VOIP, radio), videoconferencing, email, and collaboration software such Defense Connect Online (DCO). This list is not meant to be exclusive, but to focus on the tools typically used by the military.

3. Benefits

In Table 2, the Command and Control Research Program presents benefits to military operations [15].

4. Challenges

Typical challenges that are experienced in military operations can be summarized in Table 3 [15].

<ul style="list-style-type: none"> • Planning/Execution and Assessment (fielding and operating remote networks during expeditionary operations)
<ul style="list-style-type: none"> • Turing data into information and information into knowledge (creating a learning organization)
<ul style="list-style-type: none"> • Effects Based Operations (network operations support EBO)
<ul style="list-style-type: none"> • Complex problems requiring different expertise (during a critical network outage or attack)
<ul style="list-style-type: none"> • Crisis Action involving Coalition Partners (deployment of a network during disaster relief)
<ul style="list-style-type: none"> • Areas where essential knowledge is distributed (technicians or system experts not located at the NOC)

Table 2. Military Benefits of Collaboration applied to Network Operations

<ul style="list-style-type: none"> • Credibility and Trust of Participants
<ul style="list-style-type: none"> • Security Infrastructure and Policies
<ul style="list-style-type: none"> • Infrastructure Capacity and Reliability
<ul style="list-style-type: none"> • Quality and Availability of Information
<ul style="list-style-type: none"> • Usability and Interoperability of Collaboration Tools
<ul style="list-style-type: none"> • Social, Cultural, and Organizational Barriers
<ul style="list-style-type: none"> • Common Data Exchange Format
<ul style="list-style-type: none"> • Poorly Defined Roles of Participants
<ul style="list-style-type: none"> • Technology/Product Biases or Mistrusts

Table 3. Barriers to Collaboration in the Military

E. TASK FORCE ODIN (TF ODIN): REAL-WORLD EXAMPLE OF A SENSOR-SHOOTER NETWORK USING COLLABORATION

1. Background

TF ODIN started in 2006 as a classified U.S. Army program to counter the IED (Improved Explosive Device) threat and the networks that place them in Iraq. ODIN stands for Observe, Detect, Identify, and Neutralize. TF ODIN was appropriately named after the Norse god Odin who is the god of war and victory. TF ODIN operates from Camp Speicher near Tikrit [16]. TF ODIN is composed of Warrior Alpha UAVs, C-12 Cessna airplanes equipped with Electro-Optical/Infrared Sensors, Synthetic Aperture Radars and other electronic intelligence payloads, Apache attack helicopters and ground forces [17]. The sensors are comprised of the UAVs and the C-12s and the shooters are the Apaches and other ground forces.

2. Network Structure

The TF ODIN network has a robust backbone of fiber-optic cable that provides the necessary bandwidth for voice, data and video transmitted to and from the sensors, shooters and operational center [16]. The network in development since 2007 requires secure locations for the placement of network infrastructure comprised of cabling, radio towers, servers and wireless access points. Video and imagery products are typically sent to a central node for processing and fusion of data. Shooters can directly access streaming video from multiple video feeds from some UAVs and receive imagery on the One Remote Video Transceivers [18]. The UAVs and manned aircraft are controlled via separate ground control networks. The

airborne sensors transmit their data directly to the operations center by line-of-sight C-Band radio links or indirectly via a Ku-Band satellite link [16]. Shooters receive their data and communications from the Operations Center by military radio links, satellite communications links or directly from the sensor by C-Band radio links. The Operations Center, which functionally contains the Network Operations Center, transmits and analyzes data internally and to other remote processing centers via IP communication links over military channels. Data from the sensors will typically flow into a central command center. The data is processed and the information is sent to the shooter to direct them to the IED. Additionally, links exist to allow the shooter to talk/request information from the sensor if they need data that is more current without processing. This network configuration is generalized in Figure 6. Due to the nature of counter-IED operations, the network topology is dynamic. In this network, there are at least two sub-networks, the shooter segment and the sensor segment. Many times the sensor segment will be further divided into a control segment and a data transmission segment.

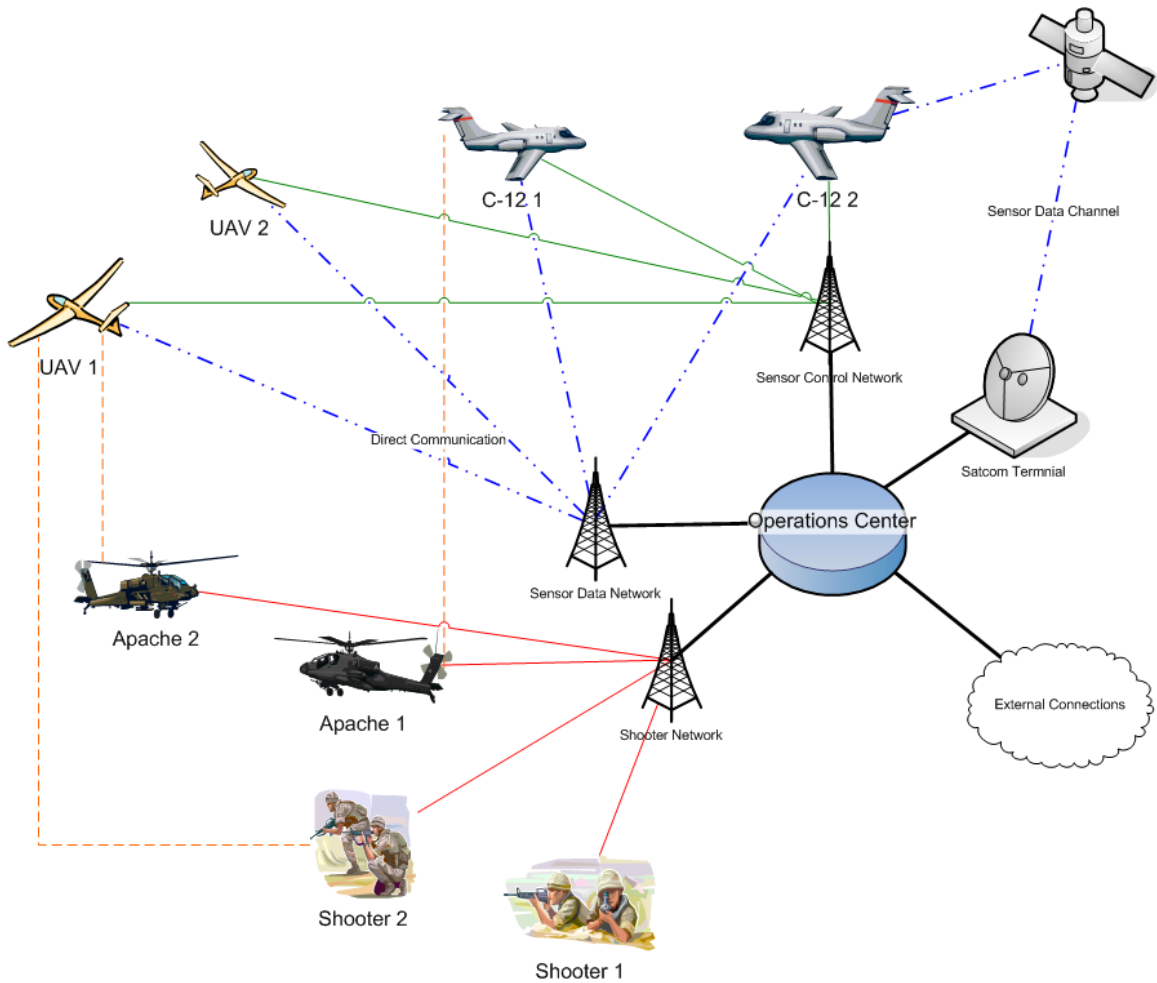


Figure 6. Conceptual Network Model for TF ODIN (From[17])

3. Operations

During a common mission, a sensor will fly ahead of a convoy looking for potential IEDs or activities that may indicate a possible attack. A sensor detects a potential IED and transmits the detection data. The data is then processed to determine the validity of the IED threat. The processing of information is performed either on board the sensor or back at the Operations Center. When a potential threat is validated, the information from the sensor (i.e., video, location, imagery) is sent to the shooter via data,

radio or voice communication links. The shooter is directed to the threat area by the Operations Center with information needed to neutralize the IED threat. The threat information is normally routed to the shooter via the Operations Center, but in a few cases the shooter can access video feeds directly from the sensor. Once the shooter is in the threat area, they will eliminate the IED threat and the convoy can proceed safely through the area.

During this process the NOC is will be maintaining healthy operational communications links for the shooter and the operations center. The sensor segment usually has dedicated personnel to maintain their network. It is common that the NOC will focus only on their network and is unaware of the status of the theater of operations network or the health of the external links. Additionally, some NOCs are not aware of the status of the radio links used by the shooters due to organizational structure. In this case it is possible to have three organizations maintain the network in the enclose sensor-shooter network.

4. Applying the TF ODIN Model to Operations and USSOCOM Expert Networks

To apply this model outside of the TF ODIN environment it is necessary to understand what the collaboration network is going to accomplish. The ultimate goal is to provide the user with an application that accomplishes the mission, does not reduce operation tempos and provides at least a satisfactory experience. When designing and operating a communications network or a collaborative network the users perspective must be included so that the network is best designed and operated to satisfy the users

needs. Collaborative networks can bring together Experts with Users, which can improve the overall effectiveness of the user/operator. One case to apply the network collaboration model (the TF ODIN model) described above is with U.S. Special Operations Command (USSCOM) Science and Technology (S&T) Branch.

For a given USSCOM operational and network model an additional communications link can be added that will allow S&T experts to leverage new technology for detection and analysis of intelligence. S&T team can apply new techniques/procedures for long-term analysis of social networks. This will allow USSCOM to connect S&T experts to forward operators that can improve their overall mission effectiveness by using system experts.

The TF ODIN model is applied to Special Operations Forces (SOF) operations due to collaborative nature of their mission. TF ODIN uses local assets on a network to detect, track and interrogate potential IED targets. SOF could use a similar model against High Value Targets (HVTs) or other special interest items. The techniques and equipment used in TF ODIN is allowing the Army to study and break into the network of the people planting IEDs by the surveillance, analysis techniques and specialized technology used. It is possible to expand some of the TF ODIN role in support of SOF operations. The coordination of communications and local Training, Tactics and Procedures (TTPs) would need to be established.

The necessary and available communications links would need to be identified so the SOF teams could get value out of a link back to the system experts at the S&T branch.

The network links that are likely to be formed will be fragile and bandwidth constricted. The network management of these links will be critical to provide a positive user experience. The S&T branch could also leverage its system experts in the support of the network management and collaborative technologies.

III. NETWORK MANAGEMENT AND COLLABORATION METHODOLOGIES

A. OVERVIEW

This chapter will start with an overview of current and future techniques of network management, application performance monitoring and application performance optimization. The chapter will end with collaboration methodologies and steps to attempt to better facilitate the collaboration process.

B. NETWORK MANAGEMENT APPROACHES FOR APPLICATION PERFORMANCE

1. ICMP and SNMP

a. *Internet Control Messaging Protocol (ICMP)*

ICMP is a basic network management protocol, described in Request For Comments (RFC) 792, that is part of the TCP/IP suite. It is a datagram based protocol that is used to determine if hosts are unreachable and the gateways used to route the data packets sent between hosts [19]. There are two common commands that are used to determine the status of the network. They are *ping* and *traceroute*. *Ping* returns the time it takes to reach a destination and *traceroute* returns the gateways that a packet travels to the destination. This is a simple overview of the implementation of ICMP, but it provides a basic management tool to determine the availability of network nodes assuming no filtering of data packets occurs.

b. Simple Network Management Protocol (SNMP)

SNMP is the Internet-standard management framework and it was developed from the OSI 7 layer network model. There are currently three versions of SNMP. SNMPv1 was the introductory version created in 1990. It is described by RFC 1157 and is the implementation of RFC 1156 (Management Information Base) [20]. SNMPv1 has five types of messages: *get-request*, *get-next-request*, *set-request*, *get-response* and *trap*. SNMPv2 was introduced in 1996 by RFC1901 [21]. SMNPv2 adds two additional messages (*response* and *get-bulk-request*) and manager applications can communicate with each other on a peer level [22]. The implementation of SNMPv2 is not backward compatible with SNMPv1. SNMPv3 was introduced in 1998 RFC2271-2275, added security measures, a framework to handle all three versions and modularization of the documentation and architecture.

SNMP is comprised of Agents, Proxy Agents and Managers. An SNMP Agent is a software module executed on an object of interest that can be queried for information from another software module. The Agent can also generate information messages base on a set of predetermined conditions, called a trap. Proxy Agents translate SNMP request to the SNMP compatible MIB and protocol from any other specialized protocol. SNMP Managers generate requests for information, manages the actions of agents and monitors SNMP message traffic. The SNMP manager is used by a Network Management System (NMS) to perform network management. There are numerous peer configurations for mangers, agents and proxies, one-to-one, one-to-many, many-to-many, and many-to-one. Figure 7 presents an example of

a one-to-many relationship with various types of SNMP agents [22]. It is important to note that a NMS can act as both an agent and a manager.

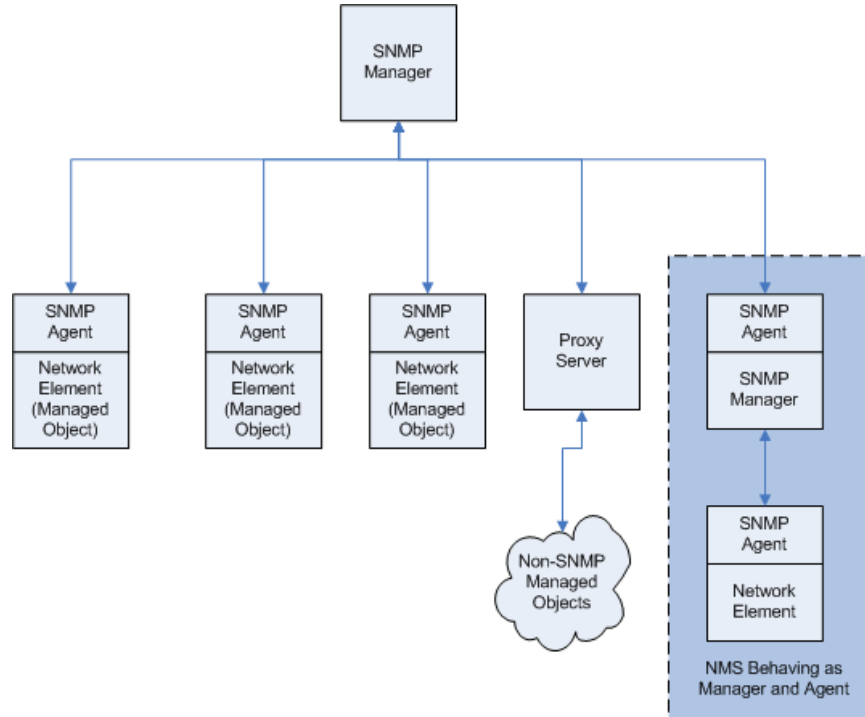


Figure 7. One-to-Many SNMP Organizational Model (From [22])

The implementation on SNMP requires a Manager to query an Agent or Proxy. The Agent will return the requested information to the Manager if it has a MIB programmed for the request. For example, a SNMP manger may query a router for how much it is being utilized and how much traffic (both number of packets and amount of bits) it has passed. The router must have a MIB that tells it how to collect the information to respond. In this case, the router responds with utilization and packets transmitted and received, but it does not have a MIB to tell it how to collect the total data it transmitted. The manufacture must program the SNMP agent on the device on what

information it can collect and how to respond including what traps it has. This reliance on manufactures limits how effectively and how widely SNMP can be implemented to monitor the network. Additionally, a host that is SNMP enabled can return sensitive information about the system to include operating system and users. This information is often protected by Network Administrators by disabling SNMP functionality on the network hosts. SNMP still remains one of the most effective ways to monitor the health and activity of the network given its limitations, but it is limited by its ability to measure applications performance since applications run on a higher level of the operations system stack and do not have agents written to monitor them.

2. Active SNMP and Network Modeling

Keshav and Sharma have approached providing QOS on a network by advanced discovery, monitoring, display, and network simulation techniques. In [1] they describe their techniques for discovery and display of the network topology and collecting statistics and simulation. Focusing on application layer performance of the network the techniques of 'Active SNMP' and network modeling are of interest. Active SNMP uses a Java applet that can monitor MIB variables for the SNMP manager. Active SNMP will operate near the MIB manager allowing for fine-tuning of performance metrics by interpreting the managed object performance and communicating the results faster. They then describe their modeling technique for networks, which is called SurREAL. SurREAL allows for the running of multiple instances of the 4.4 BSD networking kernel

virtually allowing them to simulate a virtual network that will respond to ICMP and routing requests of packets. The system administrator can test the virtual network for performance in various configurations by the prior to deployment or making changes to the live network.

3. Network Aware Nodes/8th Layer Concept

Network aware nodes are an extension of the 7-Layer OSI reference model for network communications. The 8th Layer for the Network Aware Nodes attempts to encompass all of the network management functions from the Telecommunications Management Network (TMN) [23]. The 8th layer concept extends the use of SNMP to the overall management process of the network, which attempts to provide a quality of service to the network performance.

The network aware nodes or "hyper-nodes" have the following monitoring capabilities mapped to the TMN architecture: self-diagnosis (Network Element Layer), view the sub-network topology (Network Element Management Layer), overall network performance (Network Management Layer), Quality of Service (QOS) (Service Management Layer) and negotiation of service level agreements (Business Management Layer) [23]. The hyper-nodes will monitor network performance via SNMP and will have the ability to modify their performance by using the information they gather from SNMP and by employing a memory mechanism remain aware of past network behavior. The hyper-node is also capable of forwarding on its statistics to a higher network operations center for aggregate monitoring and network performance characteristics.

The ability to monitor, affect and report on QOS is of particular interest to this thesis research. The hyper-node is network aware and communicates with SNMP agents and other hyper-nodes to adjust individual performance to achieve a higher quality of performance from the network. This in essence embodies a NOC-to-NOC collaboration to achieve higher application performance. The limitations of this version of hyper-nodes using 8th layer monitoring is the need to create an Request For Comments (RFC) and a custom Management Information Bases (MIBs) that address all the required monitoring characteristics such as QOS, Application Switching, SLA generation and negotiation to name a few [23].

4. NetFlow, sFlow, IPFIX

a. NetFlow

Described in Cisco whitepaper on NetFlow [24], NetFlow is an IP traffic flow monitoring system that creates a database on IP Traffic statistics that sends the data to a collector for reporting. NetFlow is now part of the Internet Engineering Task Force's (IETF) IP Information export (IPFIX) working group. NetFlow started the trend of IP information collection when it was introduced in 2001.

NetFlow is run from a Cisco NetFlow capable router or switch. The NetFlow datagram is a unidirectional broadcast that is directed to a specific collector. NetFlow version 1 typically monitors seven parameters:

- IP Source Address
- IP Destination Address
- Source Port Number

- Destination Port Number
- Type of Service
- Input Logic Interface (ifIndex)
- Layer 3 protocol type

This information is placed in an IP datagram as shown in Figure 8.

IP Header	UDP Header	NetFlow Header	Flow Record Data
-----------	------------	----------------	------------------

Figure 8. NetFlow Datagram

This information can be exported to a collector that can display information about the IP traffic based on Layer 3 type of service and the destination port, which can indicate the type of application being used. This information is then graphically displayed for a network manager to monitor how the bandwidth is used. NetFlow can show if the priority type of traffic, based on application port number, has enough bandwidth, which can indicate the applications expected performance. The Type of Service Field also allows the user to verify level of QOS for a specific class of service (i.e., wireless traffic) and then to adjust bandwidth allocation to maintain performance levels [24].

NetFlow is currently on version 9 and has expanded its capabilities to include monitoring of SNMP parameters, IPv6, Border Gateway Protocol version 4 (BGP4), and the use of templates to provide expandability and flexibility for future use.

b. sFlow

sFlow was developed and released in 2002 by InMon [25]. sFlow uses agents on the network that is to be monitored and run an sFlow monitoring software that collects information to be sent to an sFlow collector, such as ntop. The sFlow agent samples all the network traffic and is not tied to a specific device, but it can be embedded into switches, routers or other hardware. sFlow agents collect the traffic and package them in sFlow datagrams shown in Table 4, which are sent to the collector. The sFlow datagrams are sent to the collector embedded in a UDP packet. The collector receives and processes the traffic flow information and then displays the information for analysis.

sFlow version	IP Version	sFlow Agent IP Address	Sub-Agent ID	Switch Up-time	n Samples in datagram	n Samples
---------------	------------	------------------------	--------------	----------------	-----------------------	-----------

Table 4. 32 bit sFlow Datagram (From [26])

sFlow monitors the same parameters as NetFlow v1 plus the following parameters listed in Table 5. sFlow is configurable using SNMP unlike NetFlow.

Protocols	Layer 2	BGP 4
Packet Headers	Input/Output Priority	Communities
Ethernet 802.3	Input/Output VLAN	Path
IPX		
Appletalk		

Table 5. Additional sFlow Monitoring Parameters over NetFlow (From [27])

c. IP Flow Information Export (IPFIX) Protocol

IPFIX is the international standard protocol that standardizes the way to export information from IP Flow exports to collectors. The IPFIX Working Group has developed a MIB to monitor the exportation process and will attempt to develop an XML standard for base configuration as well as a common files structure for data storage of IP Flow data [28]. IPFIX is the protocol that is attempting to standardize the data formats for IP Flow traffic so the information can be used interchangeably. Their work continues on producing the standardized data model. The IPFIX WG has published numerous RFCs describing the standard.

5. Quality of Service by Bandwidth Allocation

There is current research that is attempting to provide QOS to the application layer by bandwidth allocations on priority of users and message type. The following areas are currently being researched and tested and the Naval Postgraduate School's Tactical Network Topology (TNT)/Mission Based Effects (MBE) experimentation program, the Air Force Research Lab and through DARPA research projects.

a. Bandwidth Allocation Auctioneering Mechanism

The auction mechanism used is based Vickrey-Clarke-Groves (VCG) auction as described in [29]. The VCG auction is also referred to as the "second-price auction" since the price paid the amount of the second-highest bid. The auction mechanism is designed to have each bidder based on their true value or priority in the system where higher

values have stronger bids. The Software Engineering Institute at Carnegie Mellon University is conducting the development of the auction mechanism. In tactical military environments bandwidth is a precious commodity that has limited resources. An auction will determine what messages will be sent based on the value of the message and the importance or value of the sender. The bidder in the auction can also send and receive messages affecting the value of the messages bid on.

The auction of bandwidth occurs on the remainder bandwidth between maximum net cycle time (the maximum network latency) and the net cycle time (the time needed to transmit messages not being auctioned). The auction process occurs cyclically but was described as every three cycles in [29]. It is important to note that the auction process generates messaging that is transmitted in the auction bandwidth period. The amount of information that can be transmitted is determined by the auctionable bandwidth (max net cycle time - net cycle time), the priority of the messages available and the priority of the bidder.

The algorithm used to determine the optimal amount of information used in the auction mechanism is a 0-1 knapsack algorithm [29]. There are x number of items to carry (data to be transmitted), each item has a certain value (data value) and the knapsack can only carry so much weight (maximum net cycle time). Using the knapsack algorithm the bidder submits their requests for the information they want to have transmitted. The higher priority the bidder is the higher the value of the bid

since the bidder priority multiplies the amount of the bid. Bidders priority levels can be changed as needed by the system or the person running the auction mechanism.

In application an auction mechanism can be deployed at a central queue where all traffic is sent to before being transmitted. There is current research being conducted by the Naval Postgraduate School using an auction mechanism with Cursor on-Target messages transmitted by a UAV in the TNT experiment test bed. Figure 9 illustrates a tactical CoT messaging network during a TNT experiment. The auction mechanism could be placed on the Air Force Research Lab (AFRL) CoT Messaging Router where it would optimize the CoT messaging traffic flow. Figure 10 illustrates the basic flow of a CoT message in a simple network.

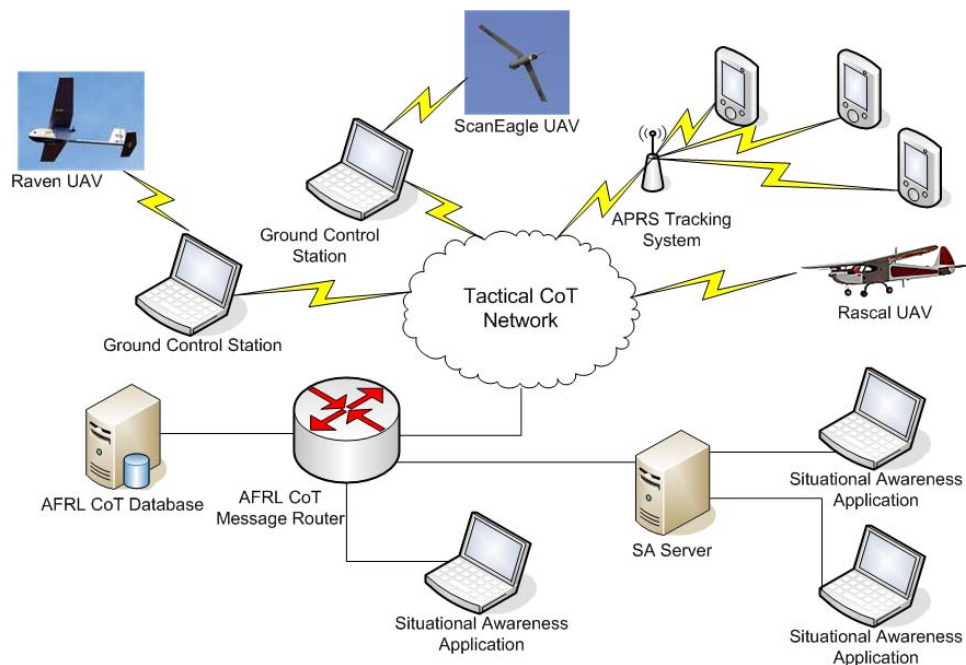


Figure 9. Deployed CoT Messaging Network (From [30])

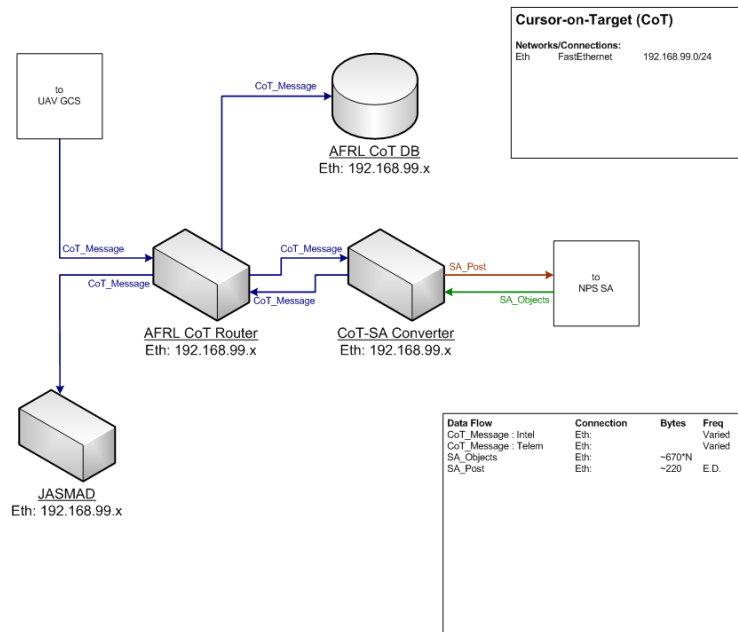


Figure 10. Basic CoT Message Flow (From [30])

b. Information Management Brokers for Cursor on Target (CoT) Messaging

The Air Force Research Lab is working on a project dubbed Marti that will act as an information management broker over a theater of operations [31]. The information manager attempts to optimize the bandwidth used to transmit Cursor on-Target (CoT) messages. CoT messages are exportable XML based message format developed by the U.S. Air Force to transmit target type information. The information manager allocates a percentage of the available bandwidth to each subscribing user based on their priority as defined by the information manager operator. The percentage of allocation and priority of the user can be changed using a specialized CoT message. This system has been tested on High Altitude, Long Endurance vehicles using various communications platforms.

c. Situation Aware Protocols in Edge Network Technologies (SAPIENT) Program/ Synthesizing Adaptive Protocols by Selective Enumeration (SYNAPSE)

The mission of the Situation Aware Protocols in Edge Network Technologies (SAPIENT) program is to create a new generation of adaptive systems that achieve new levels of functionality through situation-awareness. [32]

The approach of this program is to combine cognitive techniques (such as goal-based planning, knowledge representation and machine learning) with architectures for flexible protocol configuration (such as reconfigurable network stacks, protocol boosters, micro-protocol architectures and other extensible network architectures). The central goal of this program is to create a new generation of adaptive systems, which achieve new levels of functionality through "situation-awareness." [33]

The SAPIENT program is designed to develop artificially intelligent network control devices that can improve application layer performance using network sensors, protocol configurations and intelligent devices. One of the final two competitors that are entering into Phase 3 of the competition process is the Lockheed Martin Advanced Technologies Lab located in New Jersey. They are introducing the Synthesizing Adaptive Protocols by Selective Enumeration (SYNAPSE) device.

The SYNAPSE device acts as a bridge between two routers that are connected over a dynamically changing network that does not have reliable performance characteristics, such as in a military environment [34]. Two SYNAPSE devices are placed on the output of the routers to form the bridge. The SYNAPSE protocol framework is depicted in Figure 11.

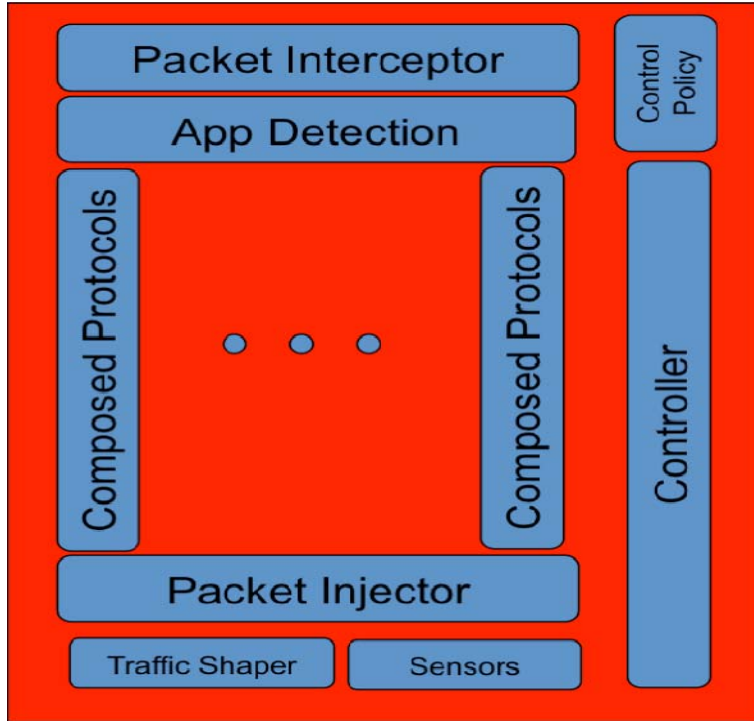


Figure 11. SYNAPSE Protocol Framework (From [34])

SYNAPSE attempts to smooth out application performance over dynamic networks by reordering and resending the application layer data packets as needed based on the application being used. While SYNAPSE is still in testing they have been configured to optimize Voice over IP, video, FTP and HTTP traffic [34].

C. COLLABORATION METHODOLOGIES

There are various modes and mechanisms that enable collaboration. This research will use a number of collaborative technologies that have been developed in house at Naval Postgraduate School by Eugene Bourakov for the TNT Network Experiments. The NPS developed applications used will be Video Conference Suite 1 (VC1), which provides video conferencing, file sharing and chat, and Observers

Note Pad, which provides persistent chat, multi-thread discussions and file sharing. Additional collaborative applications that may be used are Groove® and Defense Connect On-line®. Voice collaboration will be conducted over radio, cellular and VoIP. Table 6 shows a matrix of desired collaboration features versus the collaboration mechanisms.

Mode/Mechanism	Groove	DCO	VC1	Observers Notepad	Radio	Cellular Phone
Voice		x	x		x	x
Video		x	x			
Chat	x	x		x		
Instant Messaging	x	x	x			
File Sharing	x	x*	x	x		
Whiteboard		x				
Screen Sharing		x				
Calendars	x					

Table 6. Collaboration Methodologies Matrix

To promote effective collaboration the organization must define the mechanism it will use for each of the desired collaboration modes. It also needs to define alternate mechanism, if available, to be used if the primary tools in unavailable. Finally, there should be a moderator identified to monitor the use of the collaboration mechanism and to monitor the collaborative process. The moderator will ensure that not tool is being abused and that the collaborative process is not being dominated by an individual or group of individuals. During the collaboration process the leadership roles will frequently change depending on the situation. It is important that a moderator oversees the process so that the leadership role shifts freely and effectively.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENTATION AND RESULTS

A. TNT NETWORK TOPOLOGY

1. TNT Experiment Testbed

The Tactical Network Topology Experiment testbed is a result of a cooperative between U.S. Special Operations Command (USSOCOM) and Naval Postgraduate School (NPS). The purpose of the cooperative is to explore special operations forces (SOF) solutions to near-term and future capability gaps that have a short-fused, rapid development and testing process [35]. The TNT experiments take place primarily in Camp Roberts Army National Guard Base, Camp Roberts California, but there are numerous other sites that participate in the quarterly exercises. The TNT testbed is supported in its mission by the tactical network that allows various partners remote access and by being highly flexible and adaptable to the addition of new components. The TNT testbed allows partners from various educational institutions, industry, foreign and coalition nations and military and government agencies to operate in a collaborative environment that is unlike any other.

2. TNT OFDM Backbone

The TNT Network is used in the evaluation of networks, unmanned vehicles, advanced sensors, collaborative technology and biometric collection in a real world military environment. The network provides various layers of integration of models, tools and experimentation methods for prospective researchers. A user can connect to the TNT network via a virtual-private network (VPN), SATCOM, peer-

to-peer, or on a local segment. Sensors and unmanned vehicles can tie into the situational awareness environment by pre-defined data channels such as CoT [35].

The TNT network is monitored from the NPS Center for NETwork Innovation and eXperimentation (CENETIX) NOC during daily operations. During experimentation, the network is monitored from Camp Roberts TOC or other field site command center. The TNT backbone is comprised of a 802.16 OFDM radios that provide network services to Camp Roberts from Monterey, California over 100 miles south. The network is depicted in Figure 12. In addition to the OFDM backbone, the network has various extensions up the San Francisco Bay, across the nation and world.

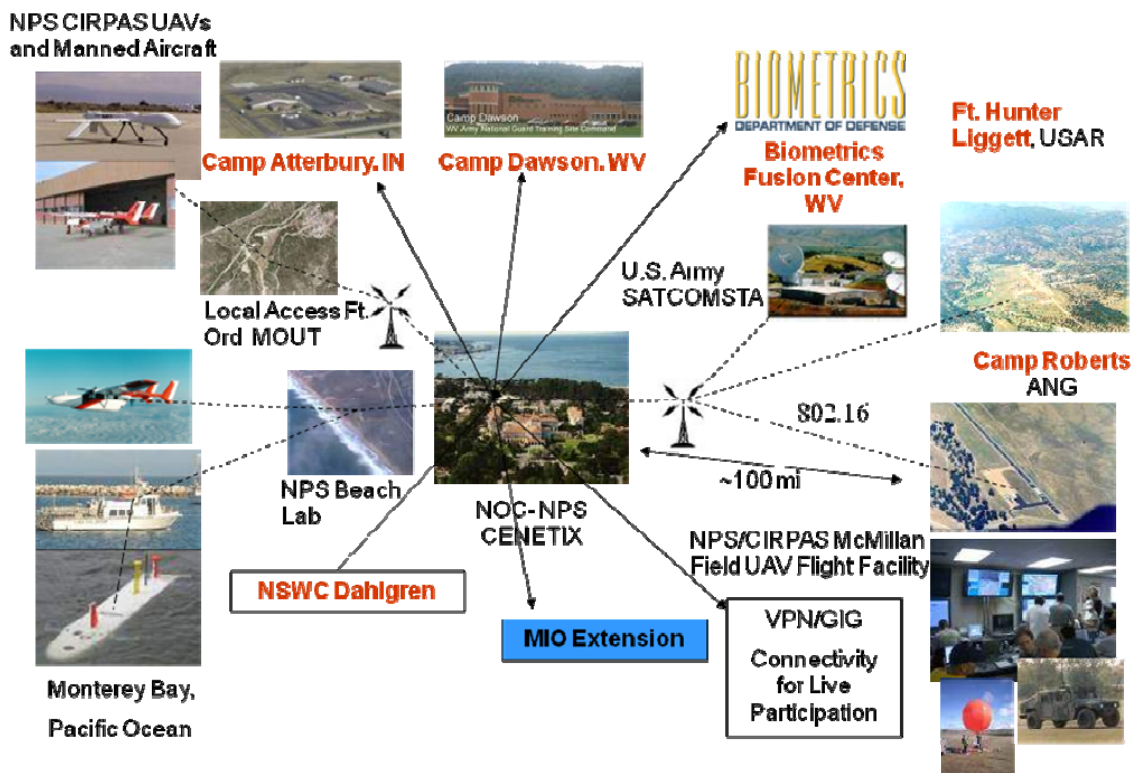


Figure 12. TNT Network Diagram (From [35])

During the experiment my role will be to act as the NOC for Camp Roberts and to provide support for additional experiments as needed. During the weeklong experiment the NOC will participate in numerous experiments attempting to monitor application and network performance and to collaborate with other parties outside the experiments listed below.

B. EXPERIMENT SCENARIOS

1. Battle Field Medical Scenario

The Battlefield Medical scenario will include the LRV NOC, the Camp Roberts (CR) Tactical Operations Center (TOC), Camp Roberts NOC, the NPS CENETIX NOC and the Rascal UAV Ground Control Station. The scenario starts with a person dismounted from the Light Reconnaissance Vehicle (LRV) that becomes injured and is in need of medical attention. That person is carrying a medical e-tag that will send an alert to the Tactical Operations Center in case of injury. The e-tag will transmit the injury location GPS coordinates and injury status via a cellular GPRS connection to the TOC. The TOC will dispatch a UAV to take imagery of the location. In this scenario, the sensor is the UAV and the shooter is the LRV and injured person with the medical e-tag. The LRV crew will send injury status reports, including a video feed to the TOC and the Medical facility, simulated at NPS. The TOC will contact a remote medical expert for advice on treating the patient. Collaboration software between all nodes will be used to treat the patient and get updated information on the injury.

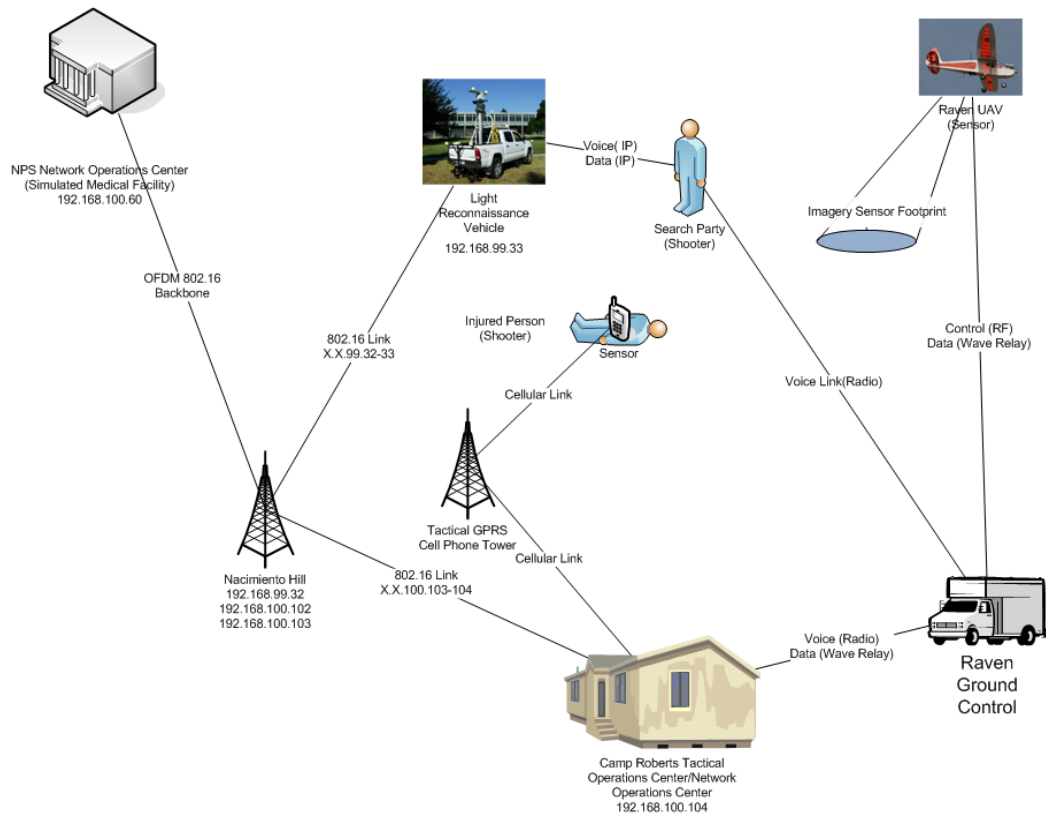


Figure 13. Battle Field Medical Scenario Network Topology

The LRV NOC will attempt to prioritize the network operations to provide the best service needed to treat the injury. Additionally, the LRV NOC will attempt to coordinate with the CR TOC/NOC and the Medical Facility (NPS) to determine application performance of the video feed and effectiveness of the collaboration software during the scenario. Figure 13 shows the sensor-shooter network configuration for the Battle Field Medical experiment. Figure 14 depicts the collaborative network that will be used for the experiment. Table 7 plots the desired collaborative tasks against the usable collaborative technologies. The collaborative tasks are the methods that each of the units would need to ensure full collaboration

and are not necessarily tied to a certain application. Situation Awareness for example, could mean views a remote application for a NOC, but it could mean knowing a unit's position for a UAV Ground Control Station (GCS).

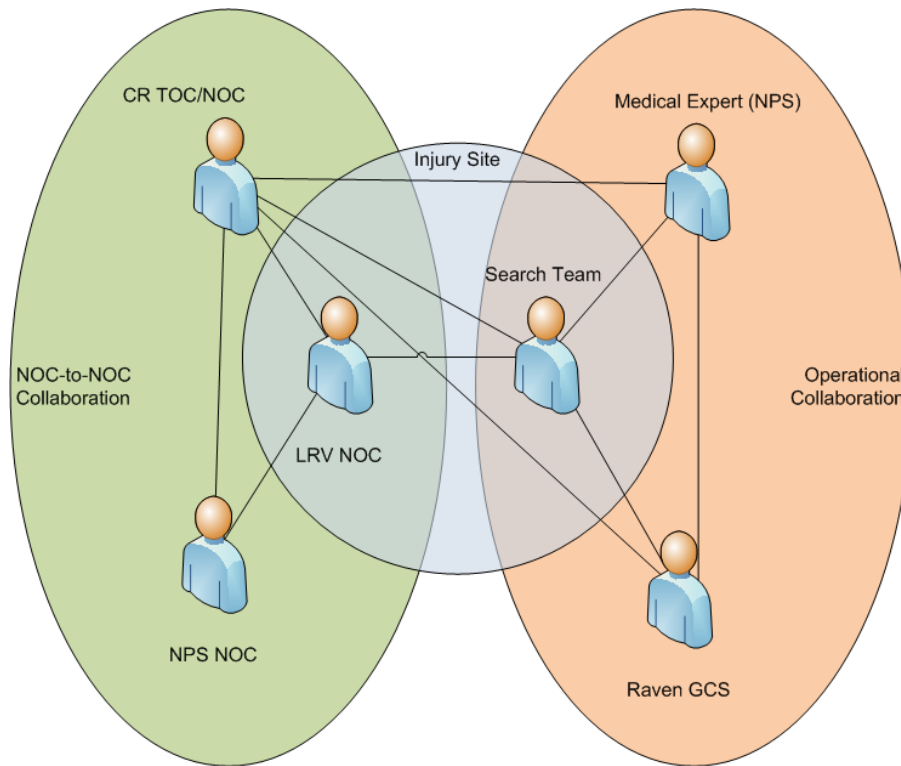


Figure 14. Battlefield Medical Collaboration Network

The collaboration network shown in Figure 12 shows three distinct collaborative areas. These areas represent the functional and operational levels that the individuals would collaborate at. There are no physical restrictions that would limit full group participation. This collaborative network is highly dependent on the social structure of the group and can quickly break down if there is poor communications and collaboration between the LRV NOC, providing support, and the Search Team, conducting operations. The placement of a LRV NOC in the operational

information flow is critical to ensure operational situational awareness is maintained by all the NOCs. In this experiment the LRV NOC and the Search team will be physically located in the same area and they will be able to conduct face-to-face communications in addition to the other collaborative tasks shown in Table 7.

	CR TOC/NOC	LRV NOC	NPS NOC	Search Team	Medical Expert	Raven GCS
CR TOC/NOC		T,F,SA, C	T,F,SA, C	T,V,F, SA,C	T,C,V,F	T,V,SA
LRV NOC	T,F,SA, C		T,F,SA, C	T,V,SA		
NPS NOC	T,F,SA, C	T,F,SA, C		T, SA		
Search Team	T,V,F, SA,C	T,V,SA			T,V,F, SA,C	T,F,SA
Medical Expert	T,C,V,F			T,V,F, SA,C		T,V,SA
Raven GCS	T,V,SA			T,F,SA	T,V,SA	

T: Talk/Voice, V: Video, C: Chat/Messaging, F: File Share,
SA: Situational Awareness

Table 7. Battlefield Medical Collaboration Matrix

2. ODIN Counter-IED Scenario

The TF ODIN counter IED experiment will attempt to recreate a typical counter-IED event using a Wave Relay™ network and Marine Corps Radios. Using the Wave Relay™ network will attempt to use a high bandwidth wireless mobile network to pass the required video, imagery, voice and other data from the sensor to the shooter. This experiment will be a proof of concept to see if a high-

speed wireless mesh network is capable of providing the required high quality network needed for advanced sensor-shooter networks.

The NOC will attempt to monitor and coordinate network operations of the Wave Relay™ network, the dismounted Marines Corps Radio Network and the TNT network so the Camp Roberts NOC, NPS NOC and the Mobile Unit. Network performance measures and application performance will attempt to be captured and relayed back to NPS from Camp Roberts. The sensor-shooter network topology for the counter-IED scenario is shown in Figure 15.

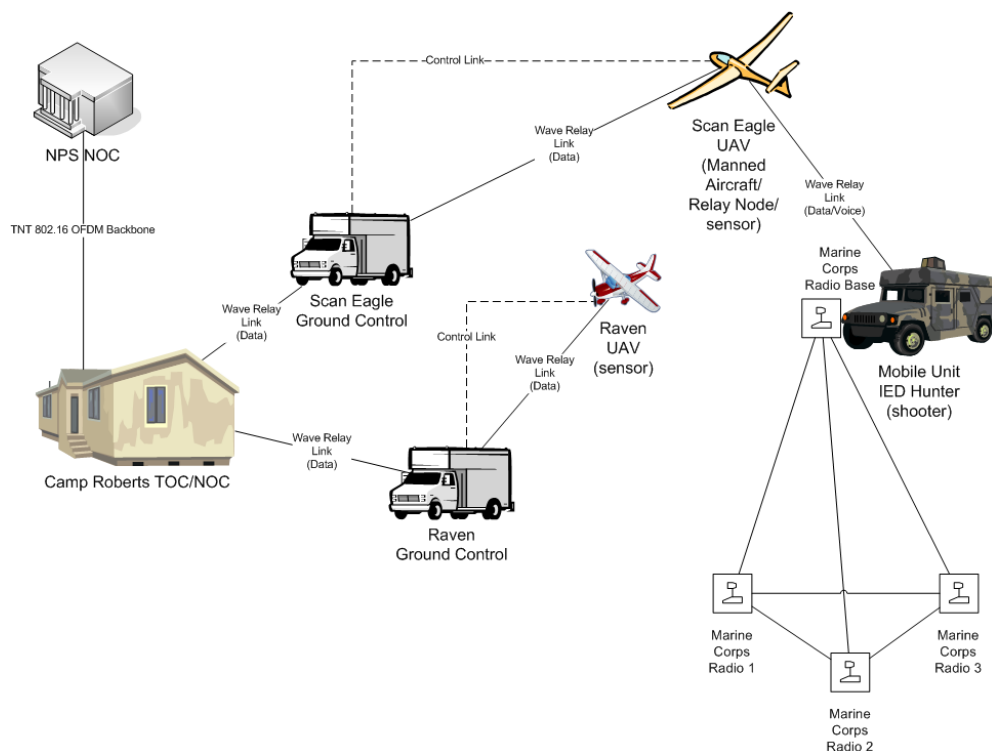


Figure 15. ODIN Counter-IED Scenario Network Topology

The collaborative environment of the ODIN experiment will be organized so that all parties can talk to each other. This is in part due to the nature of the mission

but is directly reflective of the collaborative nature of the organization, which is promoting a collaborative environment. Figure 16 illustrates the collaborative network for the ODIN Counter-IED experiment. It is important to note the LRV NOC will be collaborating in this environment even though it is not part of the formal network structure. The LRV NOC can represent any NOC on the entire network that can add increased situational awareness or knowledge to the operations of the network.

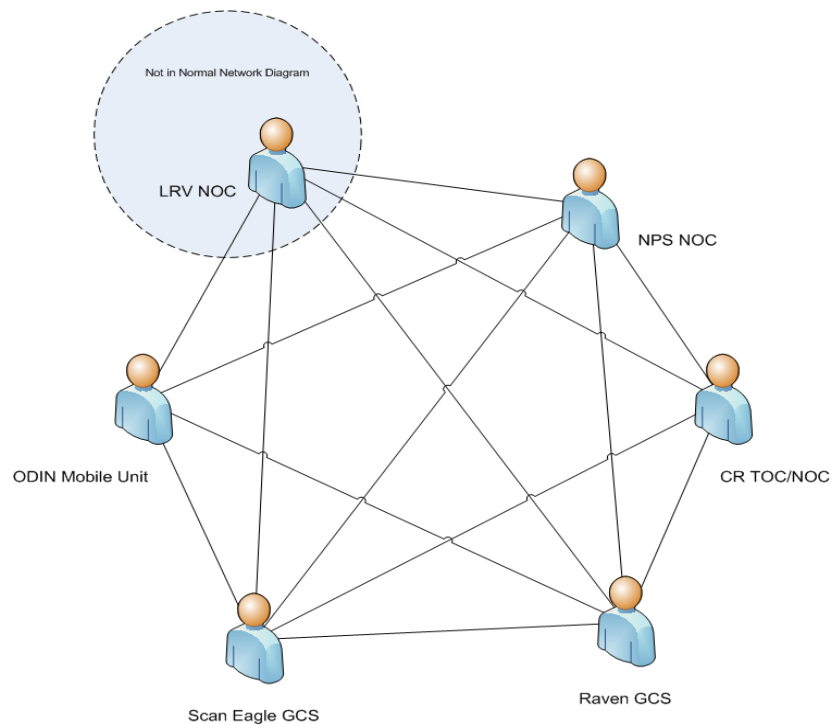


Figure 16. ODIN Counter-IED Collaboration Network

Table 8 shows the collaborative tasks that each of the units will attempt to conduct with each other. Situational Awareness (SA) is important in this exercise since the operation focus will be on UAV asset locations and the services it can provide.

	CR TOC/NOC	LRV NOC	NPS NOC	ODIN Mobile	Scan Eagle GCS	Raven GCS
CR TOC/NOC		T, F, SA, C	T, F, SA, C	T, C, F, SA	SA	SA
LRV NOC	T, F, SA, C		T, F, SA, C	T, SA	SA	SA
NPS NOC	T, F, SA, C	T, F, SA, C		C, SA	SA	SA
ODIN Mobile	T, C, F, SA	T, SA	C, SA		T, V, F, SA	T, V, F, SA
Scan Eagle GCS	SA	SA	SA	T, V, F, SA		T, SA
Raven GCS	SA	SA	SA		T, SA	

T: Talk/Voice, V: Video, C: Chat/Messaging, F: File Share,
SA: Situational Awareness

Table 8. ODIN Counter-IED Collaboration Matrix

C. EXPERIMENT MEASURES

The primary measure will be to determine the effectiveness and feasibility of NOC collaboration to provide better application performance and network monitoring. The following areas will be the focus of data collection during the experiment. Most of the data will be the collection of the collaborative process and the observation of how successful the process and mission accomplishment. The application performance monitoring will observe the current capabilities of application monitoring and what would be desired.

1. Collaboration Measures

Measuring collaboration is both subjective and objective. The U.S. Department of Agriculture conducted a

study [36] that lists several methods for measuring successful collaborative efforts in groups. For this research the following measures will be used:

- Mission success
- Commander's Intent was known
- Improve NOC level of knowledge
- Increase NOC capabilities of management
- Application statistics were distributed
- Users could effectively use their resources

While using the above areas to measure if NOC-to-NOC collaboration is effective, overall observations will be made on factors that hinder or promote collaboration in the military environments. The observations will include organizational constructs, communications procedures and communications mediums typically used in military environments. The social construct in which a collaborative environment occurs can affect the success of the collaboration as much as the mechanisms used to collaborate.

2. Application Monitoring Using sFlow

This experiment will attempt to monitor the network activity on the TNT Network during the TNT 09-2 Field Experiment in Camp Roberts California. Application layer performance will be monitored using the sFlow protocol that is has a sFlow agent, *InMon Agent 6.1*, running on a Soekris box (model net 4801). The *InMon Agent* will send the sFlow data to a Fedora host running *ntop* at 192.168.99.150. Figure 17 shows the sFlow agent-collector configuration. Ntop is configured to receive sFlow reports on port 6343.

The InMon Agent is plugged into the NPS switch, 192.168.99.1, and the Ethernet adapter was placed into promiscuous mode to capture all the traffic on the NPS TNT network that is going through the gateway.

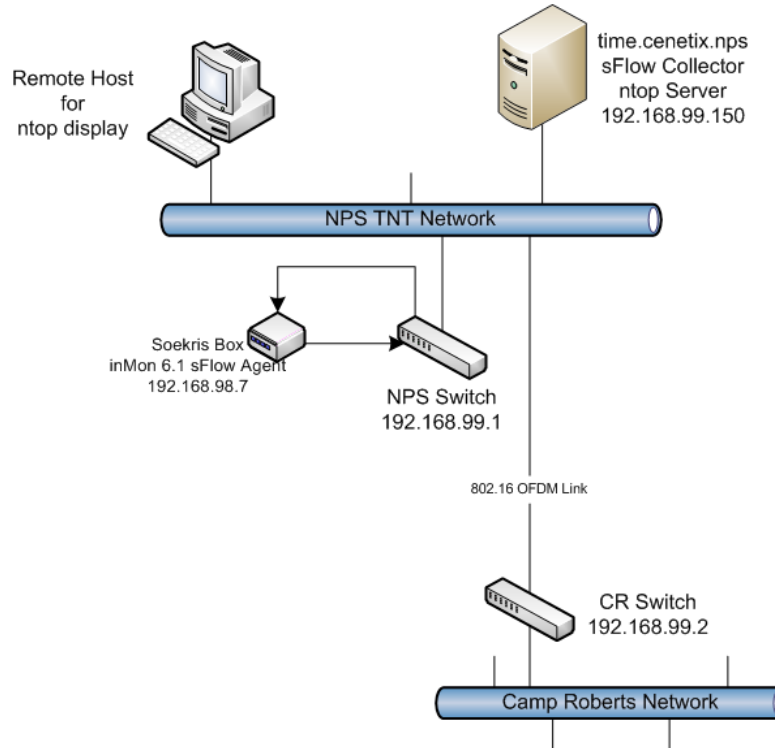


Figure 17. sFlow Agent-Collector Configuration

3. Usability of Network Applications

The overall goal for NOC-to-NOC collaboration is to improve the usability of the network applications for the user. During the experiment the usability of the network will be monitored to determine if the network is limiting the experimentation that is occurring. At this point in the research, observation of user baseline performance is the goal and determining if there are potential areas to improve network operations and apply collaboration.

D. EXPERIMENT RESULTS

1. Battlefield Medical Results

The Battlefield Medical experiment successfully used VC1, chat, file sharing via the File Repository, cellular phones and hand held radios to conduct the patient identification, diagnosis and requesting aerial reconnaissance.

The initial planning of the collaborative network and the experiment resulted in the successful completion of the experiment. During the experiment the LRV NOC, which was logged into VC1 as Chris ODA Medic, was able to coordinate with the CR TOC, BM_John, and the NPS NOC, Brian Med. Chris%20ODA%20Medic was a Search Team member on site with the LRV and he was able to facilitate network collaboration with the CR TOC and to provide situational awareness during the experiment. Figure 18 shows a picture of the VC1 in use during the experiment.



Figure 18. Video Conference for Battlefield Medic in VC1

VC1 was the primary mechanism used to collaborate for the patient assessment and treatment. VC1 was used for patient assessment from the remote site at NPS. Video, chat, and voice communications were conducted over VC1. To requests the Raven UAV to take imagery of the medic site and to deconflict mission priorities from the ODIN counter-idea experiment, radio and chat communications were used check on the status of the Raven, to verify mission tasking and to oversee the status of the experiment. NOC collaboration occurred primarily through chat.

The following observations were made from the Battlefield Medical experiment:

- Good coordination occurred between NPS, LRV, and CR Operations Centers (including command and network controls). The chat log is captured in Appendix A.
- Other network nodes responded to generated responses from LRV that indicated changes in the situational picture and overall mission focus.
- Application data and remote network monitoring of NPS was accessible at LRV. Application monitoring was accomplished with ntop from 192.168.99.105:3000. The sFlow data displayed is pictured in Figures 20 and 21 and Appendix B contains a larger amount of the sFlow data displayed by ntop. Remote network monitoring was viewed on Solarwinds Orion Webpage, 192.168.99.150, and a snap shot is shown in Figure 19.
- Unable to establish VOIP phone communications - possible configuration problem, shifted to cell phones.
- Prior planning and coordination of roles and the collaborative scenario benefited the experiment.
- Delays in Raven UAV readiness and network communications forced radio communications to be used that extended the flying window for Raven to

capture imagery. Cell phone communications were used to transmit medic site coordinates and chat was used to inform ODIN experiment of Raven situational awareness and change of mission priorities.

- Network operations occurred smoothly and the transition from IPv4 to IPv6 video streaming occurred with little trouble. Data transmission and application usage was satisfactory for the experiment. IPv6 network test was successful between the LRV Site, CR TOC and the Raven imagery server.
- It was important that the LRV NOC was close to the operations so they could maintain situational awareness and alert other network operations centers. The NOC being familiar with operations and being in the communications loop expanded to communications mechanisms of coordinating the Raven tasking by using chat and to spread the Raven UAV situational awareness to the ODIN experiment.

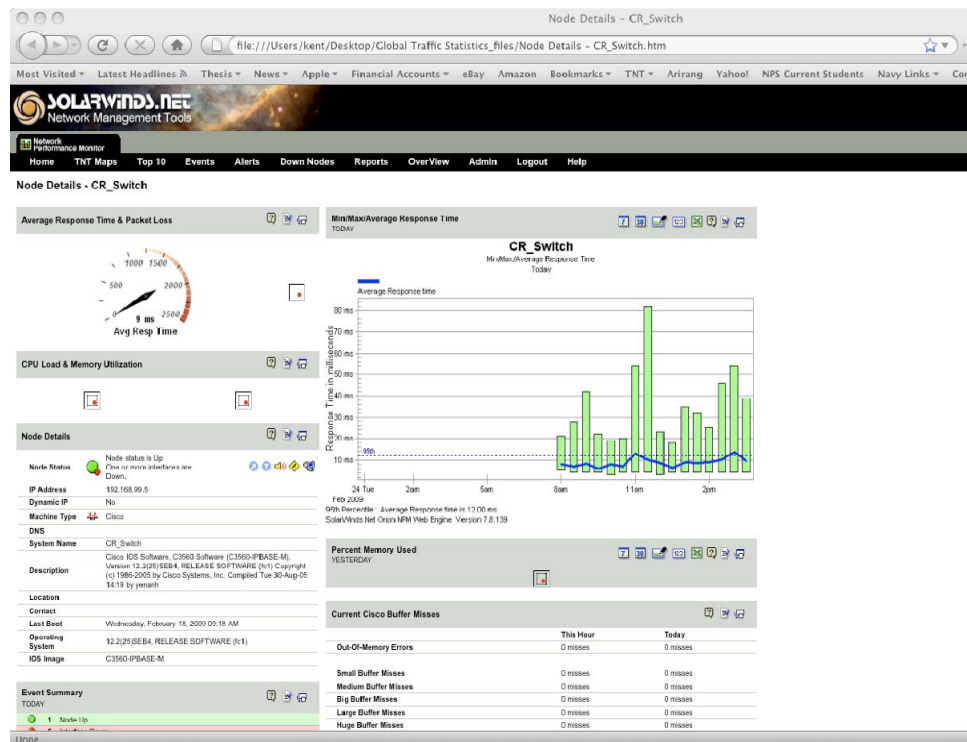


Figure 19. Network Status for Battlefield Medic

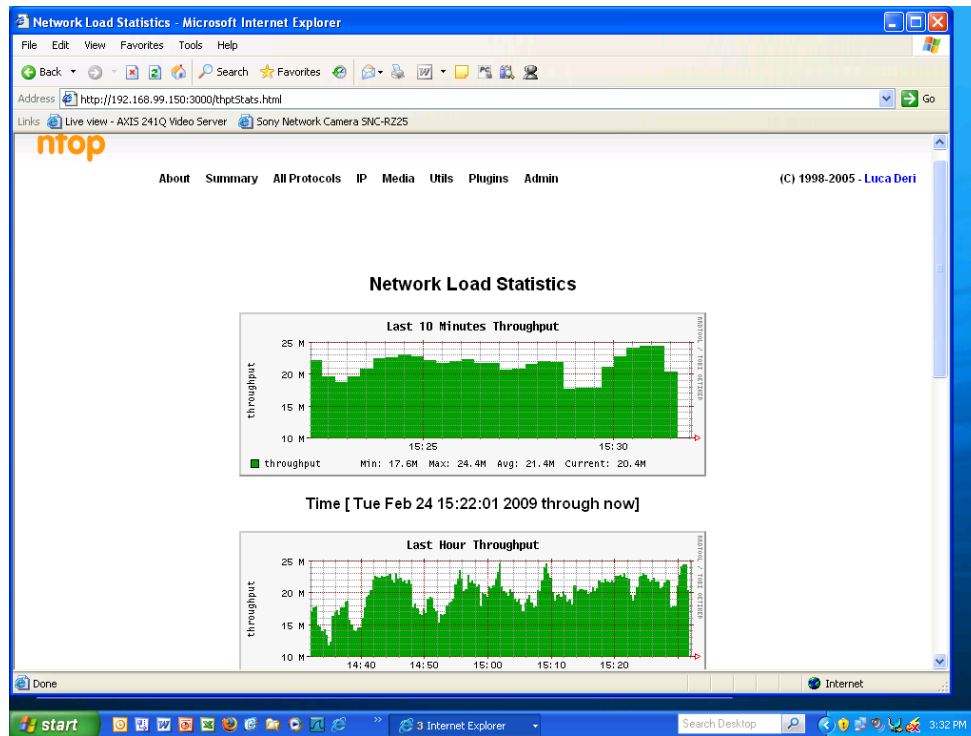


Figure 20. NPS sFlow Network Load for Battlefield Medic

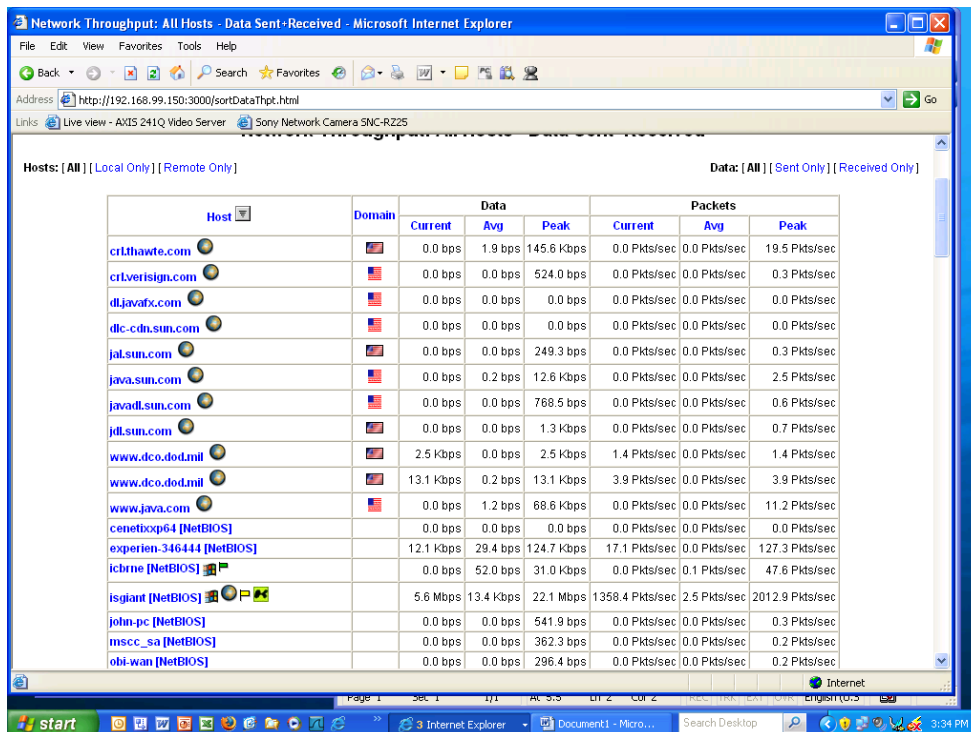


Figure 21. NPS sFlow Bandwidth Usage for Battlefield Medic

2. ODIN Counter-IED Results

The ODIN Counter-IED (C-IED) experiment was conducted at the same time as the Battlefield Medic experiment. Due to asset availability and configuration issues the Marine Corps Radios were not used and the Scan Eagle UAV was not able to act a wireless node in the sky. However, the Mobile ODIN unit was able to use the Wave Relay™ radio network to establish their communications link back to the Camp Roberts Tactical Operations Center. The Wave Relay™ network was composed of a mobile unit with a radio that connected back to the TOC via ground Wave Relay™ nodes. The ODIN Mobile Unit had both network monitor and an operations officer overseeing the experiment objectives. The NPS NOC did not have a dedicated person manned for the ODIN C-IED experiment, but the Battlefield Medic personnel were at NPS.

The ODIN C-IED was focused on sending video feeds, conducting chat, messaging, voice and file sharing during the experiment. The primary tools were VC1 and the Observer's Notepad. Collaborative communications were intermittent but for the most part successful. Successful video streamed in VC1 was not conducted due to the poor communications link from the ODIN Mobile unit and the Wave Relay™ ground segment. The low quality link was caused by geographic terrain and distance from the access point.

Application monitor was considered successful for this experiment since the LRV NOC monitored it during the same time period. The following observations were made during the ODIN C-IED experiment:

- Initial coordination between the LRV NOC and the ODIN NOC was poor due to the technical issues occurring at the ODIN Mobile site.
- The ODIN NOC and ODIN Mobile did not respond to communications checks conducted via chat in VC1 or the Observer's Notepad. See Appendix A for a record of all the TF ODIN chat records.
- Initially, neither ODIN NOC nor ODIN Mobile responded to the injection of the medical emergency and only had situation awareness of their environment.
- Once communications was established between the ODIN NOC and ODIN Mobile the collaborative process and situational awareness improved. ODIN Mobile communications and movement status was frequently updated and ODIN Mobile was able to gain situational awareness on the flight status of Raven.
- ODIN Mobile was reached using multiple paths of communications (radio, chat and cell phone) to inform them of the tasking status of the Raven and to let them know that Raven was going to fly. The radio was the quickest and most effective path due to ODIN Mobile support driver was listening on flight communications and passed along the message.
- ODIN NOC updated situational awareness frequently on the communications status of ODIN Mobile. Screen captures were uploaded to Observers Notepad to test the file sharing capability. A sample file is shown in Figure 22.
- In remote and austere environments it is critical to have multiple communication mechanisms to ensure communications and collaboration are successful.
- The initial focus of the ODIN NOC on their network limited their ability to maintain situational awareness of the entire experiment. It is important that NOC are actively looking at the entire operation they are supporting so they can optimize their network performance.

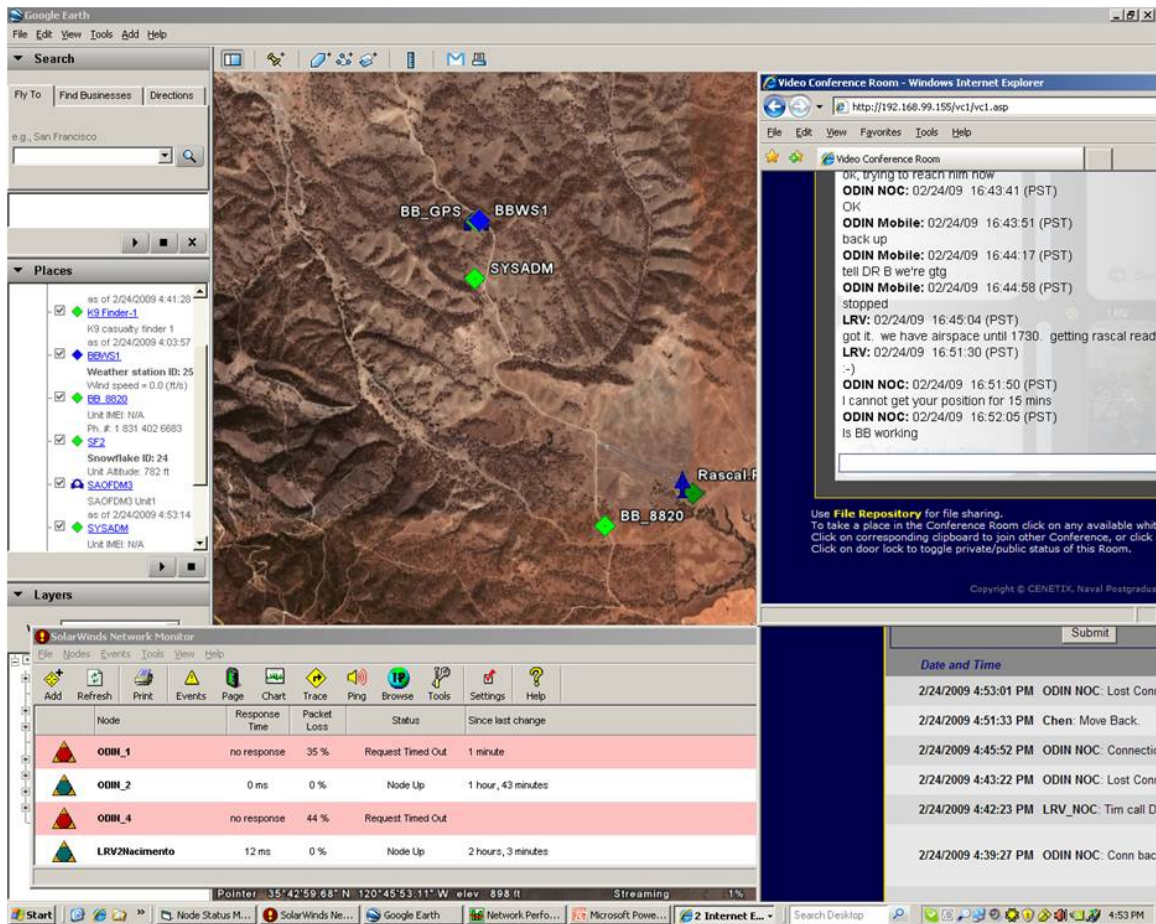


Figure 22. ODIN Mobile Network Status, Loss of Link

3. Overall TNT 09-2 Experiment Results

During the weeklong experiment at Camp Roberts, two experiments involved the CR NOC providing network and situational awareness support. These two experiments highlighted areas that play critical roles in the success of NOC collaboration.

a. Parafoil Drop and Control Experiment

CR NOC was acting as recording and monitoring agent for the parafoil drop experiment. During this experiment, CR NOC was responsible for recording

significant operational events of the experiment in Observer's Notepad. The records of those events are displayed in Appendix A. CR NOC was not directly positioned (physically or logically) in communications path. The experiment lead was located in a room to the left of CR NOC and the Air Boss, who controls air operations, was in a room to the right of CR NOC. This location required the CR NOC to actively seek out information on significant activities, such plane take-off, parafoil drop and target drop. There were two times were CR NOC had to directly ask and confirm the status of a significant act with the experiment lead. The CR NOC had to actively search for information to maintain the situational awareness of the experiment so accurate logs could be recorded.

The significance of this experiment was to highlight the need for the NOC to be in the line of communications on operational events so they can interpret and resend that information to other NOCs of the operational status as it applies to NOC and the completion of the commander's intent.

b. Network Monitoring of Redline AN-80i Radio.

During the network monitoring of the Redline AN-80i radio the LRV was deployed to a remote location and extended the TNT Tactical network with the AN-80i radio, which is also an 802.16 radio that has SNMP enable management functions. The goal of the experiment was to establish the radio link, monitor the radios and explore the management functionality of the radios. The LRV had an experienced SolarWinds and network management operator. The

Redline Radio monitoring was occurring back at the CR NTOC. The CR NTOC has military communications officer who was familiar with network management, but not experienced with the software.

During the experiment the LRV operator was able to collaborate using VCI and phone communications with the CR TOC on how to configure SolarWinds to remotely monitor the radios. The LRV was able to verify the configuration and monitoring of the radio locally and then record screen shots, which were uploaded to the File Repository. Once the LRV operator conducted successful monitoring, the knowledge of how to configure SolarWinds was passed to the CR TOC operator. Figures 23 and 24 show the configuration and initial monitoring capabilities of the Redline radios conducted during the experiment.

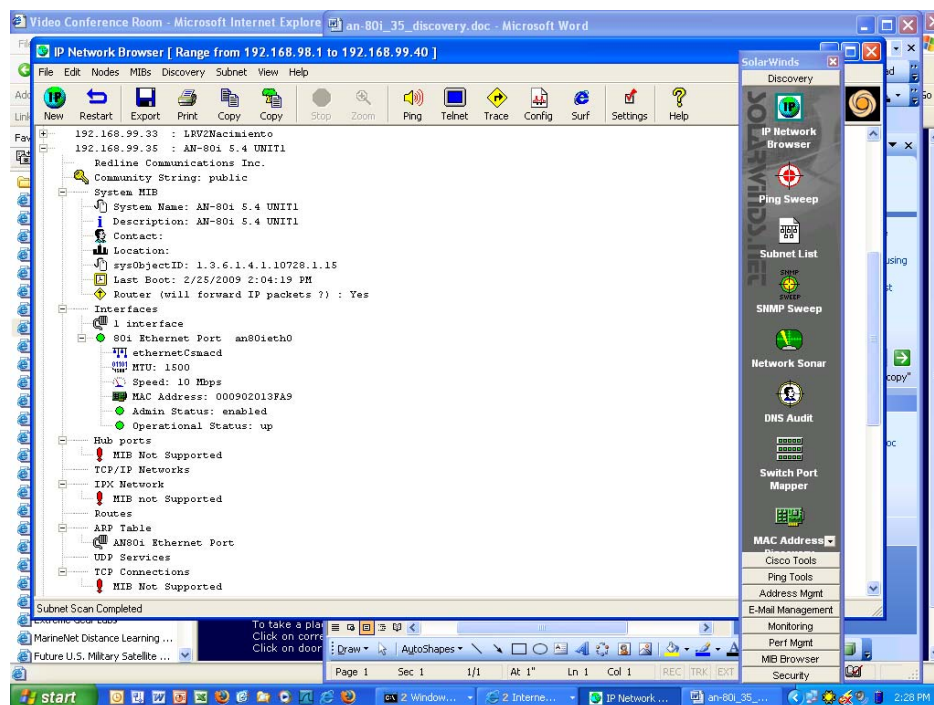


Figure 23. Redline AN-80i Network Discovery

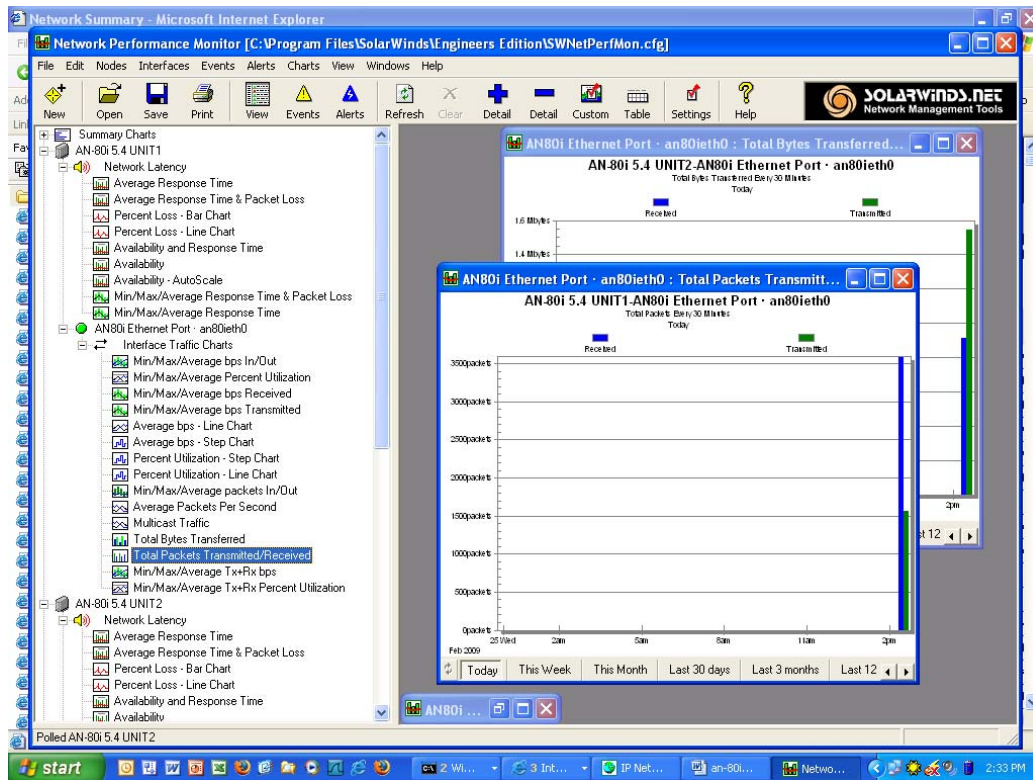


Figure 24. Redline AN-80i Initial Performance Monitoring

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This research looked at Network Operations Center (NOC) collaboration as a means to improve application layer performance of a network while meeting the commander's intent of a military mission. The focus was on a sensor-shooter network that would accomplish a military task that would most likely involve the use of firepower. During the experimentation phase of the research it became apparent that NOC collaboration could be applied to all aspects of military operations to include administrative, defensive, offensive and other than military operations such as disaster relief. The following areas will address the findings of this research. If these areas can be implemented in the operation of military networks the overall effectiveness of military operations can be improved.

1. NOC-to-NOC Collaboration

NOC collaboration allows for the transfer of knowledge from more experienced NOCs to less experienced NOCs that are geographically separated. The use of messaging, voice communications and situational awareness of the network allows NOCs to effectively collaborate. Situational awareness (SA) of a network is more than just remote monitoring of application of network health. SA can be used to allow remote access to another machine or window. Remote access can provide a rapid transfer of knowledge by watching and doing more complex tasks of network management.

The sensor-shooter network needs to be viewed as a network of networks with multiple NOCs in the holistic network. The authority on monitoring and optimizing the networks will constantly change based on the mission being accomplished and the commander's intent. It is important to have a moderator to oversee the collaboration and management efforts. The moderator needs to ensure the one NOC does not dominate the process and disrupt operation of the entire network.

NOCs need to maintain operational SA so they can optimize their network. The onus is on the NOC to ensure they maintain operation SA and can articulate needed changes to other NOC and the overall status of the network to the commander.

A NOC needs to focus is on usability of network applications not just health of the network. In the military environment the network health can be assumed to a changing constant that operations must adjust too. While the NOC will work to create the most robust network it can, areas of military operations create rapidly changing and very fragile networks. The primary focus should be on application performance. If a NOC can monitor and modify the performance of applications of the network then they can improve the usability of the network.

Inherent in all military collaborations, multiple methods of communications are essential to maintain a collaborative effort. When NOC collaborate they should attempt to impact the network as little as possible and potential use alternate paths of communication to protect

the user experience. It is not acceptable to tax the network resource to maintain collaboration at the expense of the user.

A primary tool that NOCs use to manage and display the health and operation of the network is Network Management Systems (NMS) such as SolarWinds Orion or SYS Network Solutions dopplerVUE. These tools could be expanded to include a collaboration functional that would allow NOCs to communicate and share information from a common platform using existing protocols that would not burden the network with excessive traffic. A NMS with collaborative functions could potentially increase the operational effectiveness of NOC and improve their knowledge transfer ability.

2. Application Monitoring and Performance

Application monitoring is fundamental to improve the overall application layer performance of a network. To dramatically improve the performance of the network the flow of application traffic needs to be able to be modified or shaped to match a fixed bandwidth allotment. The ability to reshape or prioritize traffic flows based on specific applications will be crucial to improving the application layer performance over a disadvantaged network.

The use of modern mainstream application flow monitors (i.e., sFlow or NetFlow) is primarily designed for protocol traffic monitoring, but they allow filtering on ports that can be associated with applications. The configuration of port filtering can be time intensive and may be inaccurate depending on the implementation of the ports used by the application. The only way to guarantee accurate application monitor is to perform a packet inspection, but

this can be resource intensive and disrupt an already fragile network. sFlow as used in this experiment, provided insight on application and bandwidth usage, but did not have a fine enough granularity to optimize the application performance.

To improve application performance an agent will need to be used to shape and monitor traffic. An agent such as the SYNAPSE device or a bandwidth auctioning mechanism would benefit the NOC operations and user-level performance. These agents would need to network monitors that could alert them of changes in the network performance. The network monitor should be aware of its condition and the condition of the surrounding network. In this case a hypernode or an 8th Layer node would provide the best network sensor information to the flow-shaping agent. Ideally, the flow-shaping agent would be able to present in performance data to the NOC and it could be dynamically changed to meet new operational requirements.

3. Meeting the Commander's Intent by Maintain Situational Awareness

Any group that wants to meet the commander's intent must have some sort of situational awareness on the entire operations to function effectively in a Network Centric Warfare (NCW) environment. For a NOC to maintain situational awareness of the overarching mission they need to be directly integrated into the Operation Center. The NOC needs to be logically and physically located where they can monitor operations and directly assess network and application layer performance. The NOC representative that is in the Operations Center workspace will be able to

translate the operational picture to local servicing NOC and to other NOCs on the global network.

The operational mindset of networks only a service provider must change so that they are considered an operational component of the entire organization. This is a premise underlying NCW and it is a key pillar in Information and Effects Based Operations. The commander must also require that the NOC is maintaining its situational awareness and become operationally focused. The NOC must also seek out operational interactions so they can ensure the network is optimized instead of sub-optimizing each local component.

Changing the physical and logical position of the NOC will improve the collaborative capabilities of a NOC and it will enable it to disseminate the commander's intent to the entire network.

B. FUTURE WORK

There are a few potential areas of further research in this topic that reside in the social and technical realms. The first area deals with the social and organization construct of the NOC in relation to the Operations Center. A study of various organizational constructs can be focused to determining the best way to operationalize the network support function. This study can look at different organizational sizes and types and attempt to determine if there is an architectural approach to the organization design.

The next potential area is a technical study of bandwidth allocation devices or flow shaping devices on the

application layer performance and user level operability of a disadvantaged network. The technical study would look at levels of performance improvements of limited networks with flow shaping devices against networks without the device. This will determine the effectiveness and potential of the devices to improve military edge networks.

One last area of future research is the identification of necessary collaborative functions a network operations center needs to collaborate. This area could explore what tasks a NOC needs to collaborate (i.e., chat, desktop sharing, voice and remote management). Once the functional collaboration areas are identified they could be integrated into a NMS. The integration, user display and industry cooperation would aid in bring this capability to mainstream usage for geographically separated organizations.

APPENDIX A: CHAT DATA CAPTURES

A. BATTLEFIELD MEDICAL CHAT DATA

BM_John: 02/24/09 14:30:31 (PST)Did you get this?
Brian Med: 02/24/09 14:31:06 (PST)I got it.
BM_John: 02/24/09 14:30:50 (PST)Chris.....
Brian Sqd Av: 02/24/09 14:31:44 (PST)I got it too
(Brianx2)
BM_John: 02/24/09 14:40:43 (PST)Chris, you up?
Chris ODA Medic: 02/24/09 14:44:18 (PST)This is the LRV
with an ops check. request all stations respond.
Brian Med: 02/24/09 14:45:01 (PST)I got you on both mine
BM_John: 02/24/09 14:58:44 (PST)start from beginning since
we have chat
BM_John: 02/24/09 14:58:47 (PST)ENDEX
BM_John: 02/24/09 14:58:50 (PST)STARTEX
Chris%20ODA%20medic: 02/24/09 15:00:01 (PST)Event 1: A
patrol sized element from the ODA has left its firebase and
is actively searching for members in an IED network.
During the course of the mission one of the patrol members
spots a tribal leader he recognized from a council he
attended a few weeks ago.
Chris%20ODA%20medic: 02/24/09 15:01:14 (PST)Event2: That
tribal leader is a key figure in making in the success of
the FID mission and with helping the ODA defeat the IED
network. The patrol stops to talk to him and see if they
can gain any information. The patrol knows that gaining
and keeping the leader's trust is very important to mission
success.
BM_John: 02/24/09 15:00:49 (PST)B-
BM_John: 02/24/09 15:00:54 (PST)B-Team standing by
Chris%20ODA%20medic: 02/24/09 15:01:49 (PST)During the
course of the conversation they learn that the leader's
only daughter is very ill and is in need of medical help
soon. He has heard stories of the ODA's medical prowess
and wishes that his people have the same level of care.
The patrol seizes on the opportunity to help his daughter.
Chris%20ODA%20medic: 02/24/09 15:03:01 (PST)Event 3: The
ODA medic, a seasoned and experienced person, examines her
and determines that he needs additional, specific
information about the local region in order to diagnose the
girl's condition.
Chris%20ODA%20medic: 02/24/09 15:04:07 (PST)Event 4: He
radios back to the watch officer at the ODA's firebase via

VHF radio for additional help regarding the diagnosis he needs to make.

Chris%20ODA%20medic: 02/24/09 15:04:56 (PST)Event 5: The ODA watch officer (Odell) will then contact the MF (Real) and the B-Team (Dobrydney) over his collaboration tool (VC1 video conferencing tool: video/voice and chat) to relay the medic's questions. The collaborative group of the MF, the ODA watch officer, and the B-Team senior medic will confer and ultimately decide that the daughter needs a video consult.

BM_John: 02/24/09 15:04:33 (PST)Odell, what do you have?

Chris%20ODA%20medic: 02/24/09 15:05:51 (PST)AN tribal elder's girl needs medical consult via VC1

BM_John: 02/24/09 15:05:38 (PST)What seems to be the problem with her?

Chris%20ODA%20medic: 02/24/09 15:06:58 (PST)She is exhibiting symptoms I am unfamiliar with and need a MD to look at

BM_John: 02/24/09 15:06:43 (PST)Roger, Med Facility wathc, are you on the net?

Brian Med: 02/24/09 15:07:32 (PST)Med Facility watch standing by...

Chris%20ODA%20medic: 02/24/09 15:08:21 (PST)Event 6: Begin Medical Consult. (Odell points the camera at the mannequin) From there, the collaborative group can observe her with a video camera and the MF (Real at CENETIX) can observe and ask ODA medic (Odell) questions and to perform tasks.

BM_John: 02/24/09 15:07:53 (PST)Pls respond to the ODA's issue

Chris%20ODA%20medic: 02/24/09 15:08:46 (PST)I will move my web cam so you can exmine the patient

Brian Med: 02/24/09 15:08:57 (PST)MD standing by for camera consult

Chris%20ODA%20medic: 02/24/09 15:10:28 (PST)Her vitals are normal. She has a severe rash that is spreading. Purple in color. I will show you

Chris ODA Medic: 02/24/09 15:10:29 (PST)test situational awareness message. possible change in tasking

BM_John: 02/24/09 15:11:05 (PST)say again?

Chris%20ODA%20medic: 02/24/09 15:11:52 (PST)What do you think doc?

Brian Med: 02/24/09 15:11:47 (PST)Diagnosis is for Binstockitis

BM_John: 02/24/09 15:11:41 (PST)what do we need to do for it?

Chris%20ODA%20medic: 02/24/09 15:12:26 (PST)What is the treatment

Brian Med: 02/24/09 15:12:35 (PST)Treatment is to dress area and keep clean. Take two aspirin every 8 hrs.

Chris%20ODA%20medic: 02/24/09 15:12:53 (PST)vitamin M or what?

BM_John: 02/24/09 15:12:25 (PST)motrin

BM_John: 02/24/09 15:12:30 (PST)man

Brian Med: 02/24/09 15:13:04 (PST)Motrin is a good substitute.

Chris%20ODA%20medic: 02/24/09 15:13:29 (PST)We'll need to fly out some meds for her

BM_John: 02/24/09 15:12:52 (PST)MEDEVAC?

BM_John: 02/24/09 15:13:04 (PST)...or fly out meds?

Brian Med: 02/24/09 15:13:40 (PST)Fly out meds should suffice.

BM_John: 02/24/09 15:13:20 (PST)Squadron stand by for mission request

Chris%20ODA%20medic: 02/24/09 15:14:24 (PST)Doc do you need to see her in your office or can I administer the treatment?

Brian Sqd Av: 02/24/09 15:14:10 (PST)sqd watch standing by

BM_John: 02/24/09 15:15:07 (PST)Can the medic administer meds in the field?

Chris ODA Medic: 02/24/09 15:16:24 (PST)use control-print screen, then you can copy to word

Chris ODA Medic: 02/24/09 15:16:28 (PST)

BM_John: 02/24/09 15:16:51 (PST)...Sqd standby for meds delivery to the ODA

Brian Sqd Av: 02/24/09 15:17:28 (PST)I have an alert 15 that can support that mission

Chris%20ODA%20medic: 02/24/09 15:18:42 (PST)I can send a file with the LZ layout for the helo

Brian Sqd Av: 02/24/09 15:18:45 (PST)Send your LZ file

Chris%20ODA%20medic: 02/24/09 15:20:19 (PST)Uploaded LZ file

BM_John: 02/24/09 15:19:55 (PST)Where is the file going?

Chris ODA Medic: 02/24/09 15:21:18 (PST)LRV sees file

Brian Sqd Av: 02/24/09 15:21:21 (PST)Revd File

Chris%20ODA%20medic: 02/24/09 15:21:54 (PST)What is the ETA for the helo

Brian Sqd Av: 02/24/09 15:21:47 (PST)15 Mins

Chris%20ODA%20medic: 02/24/09 15:22:22 (PST)Roger, 15 minutes

Chris%20ODA%20medic: 02/24/09 15:23:09 (PST>Hello is landing.

Brian Sqd Av: 02/24/09 15:22:58 (PST)rgr
Chris%20ODA%20medic: 02/24/09 15:23:19 (PST)Received meds
Chris%20ODA%20medic: 02/24/09 15:23:23 (PST)Thanks doc
Chris ODA Medic: 02/24/09 15:24:05 (PST)test
message....hostile file in northern area, IED attack
occurring prioritize network assets to northern sector.
stations acknowledge
Brian Med: 02/24/09 15:23:58 (PST)request you schedule
patient for follow up in 1 week
BM_John: 02/24/09 15:23:38 (PST)B-Team Ack
BM_John: 02/24/09 15:23:52 (PST)ENDEX
BM_John: 02/24/09 15:33:51 (PST)hooahh!!!
BM_John: 02/24/09 15:34:27 (PST)fun fun fun fun
Brian Sqd Av: 02/24/09 15:35:43 (PST)to confirm cancel
DCO?
BM_John: 02/24/09 15:35:30 (PST)CANC DCO for now
BM_John: 02/24/09 15:36:19 (PST)Sir, you are breaking up,
cant hear
Brian Sqd Av: 02/24/09 15:37:17 (PST)John you there?
BM_John: 02/24/09 15:37:06 (PST)Am here, could not hear
Brian Sqd Av: 02/24/09 15:37:51 (PST)The Bord is heading
to the TOC 5 min
BM_John: 02/24/09 15:37:40 (PST)copy,
Brian Sqd Av: 02/24/09 15:38:20 (PST)Starting Battlefield
med without Rascal
Chris: 02/24/09 15:38:40 (PST)John can't talk to you but
can see you. I can also hear you
BM_John: 02/24/09 15:38:10 (PST)correct
Chris ODA Medic: 02/24/09 15:39:14 (PST)you can try
refreshing the windows
Chris ODA Medic: 02/24/09 15:39:45 (PST)you may have to
re-log in after this
BM_John: 02/24/09 15:39:25 (PST)how is this?
Brian Med: 02/24/09 15:48:10 (PST)Que?
BM_John: 02/24/09 15:47:54 (PST)Running injects on a
scenario
BM_John: 02/24/09 15:48:04 (PST)I hear those guys talking
right now
Brian Med: 02/24/09 15:48:34 (PST)OK
BM_John: 02/24/09 16:08:38 (PST)antenna suddenly moved fwd
after three min delay
Brian Med: 02/24/09 16:10:39 (PST)Injection!
Brian Med: 02/24/09 16:10:47 (PST)Agent Id 25
BM_John: 02/24/09 16:12:42 (PST)activated three times
medical injection
BM_John: 02/24/09 16:15:41 (PST)confirmation on injection

Brian Med: 02/24/09 16:17:54 (PST)Out Back RHR ?'s

B. TF ODIN CHAT RESULTS

MIO Expert: 02/24/09 13:27:15 (PST)Test- Chen, see me now?
LRV_NOC: 02/24/09 14:48:42 (PST)This is LRV with an OPS check. Request all stations respond
LRV_NOC: 02/24/09 14:56:01 (PST)test test
LRV_NOC: 02/24/09 15:10:50 (PST)test to all stations
LRV_NOC: 02/24/09 15:17:44 (PST)test
LRV_NOC: 02/24/09 15:53:31 (PST)test message please respond
ODIN NOC: 02/24/09 16:01:58 (PST)I cannot hear you
ODIN NOC: 02/24/09 16:02:18 (PST)I got the picture with coordinates and distance to NOC
ODIN NOC: 02/24/09 16:03:20 (PST)I think it's better to use chat
ODIN NOC: 02/24/09 16:04:51 (PST)You are still connected
ODIN Mobile: 02/24/09 16:07:32 (PST)reconnected at new location
ODIN Mobile: 02/24/09 16:07:49 (PST)waiting on raven to launch
ODIN NOC: 02/24/09 16:08:19 (PST)Lost connection to Tim for few second
ODIN NOC: 02/24/09 16:08:23 (PST)Up again
ODIN Mobile: 02/24/09 16:09:15 (PST)ok, is the rascal uav launching
ODIN NOC: 02/24/09 16:09:27 (PST)not yet
ODIN Mobile: 02/24/09 16:11:32 (PST)let me know when it takes off
ODIN NOC: 02/24/09 16:12:20 (PST)ok
ODIN Mobile: 02/24/09 16:13:30 (PST)ask when the rascal is going to take off
ODIN Mobile: 02/24/09 16:13:37 (PST)also, on the move again
ODIN NOC: 02/24/09 16:13:55 (PST)ok
ODIN NOC: 02/24/09 16:15:14 (PST)I'll as Dr. Bordetsky when available, no one else knows it
ODIN NOC: 02/24/09 16:15:27 (PST)And I still see it off
ODIN Mobile: 02/24/09 16:15:29 (PST)can you see the webcam?
ODIN NOC: 02/24/09 16:16:00 (PST)yes I can
ODIN Mobile: 02/24/09 16:18:28 (PST)will not be able to use the raven have to wait for the rascal
ODIN NOC: 02/24/09 16:20:30 (PST)OK. Nobody knows about Rascal, All they say it should take off soon

ODIN NOC: 02/24/09 16:22:47 (PST)It'll be in the air in 15 minute
ODIN Mobile: 02/24/09 16:22:48 (PST)ok, not sure if we're going to get much more data then, no our way back
ODIN NOC: 02/24/09 16:23:56 (PST)ok
LRV: 02/24/09 16:24:10 (PST)rascal is about to go airborne
ODIN_Observer: 02/24/09 16:25:08 (PST)NOC do you use Ixchriot to measure throughput.
ODIN NOC: 02/24/09 16:25:59 (PST)We could not set Marine Radios
ODIN_Observer: 02/24/09 16:25:57 (PST)Check.
ODIN Mobile: 02/24/09 16:30:08 (PST)stopped now, pls plot our location
ODIN NOC: 02/24/09 16:30:18 (PST)ok
ODIN Mobile: 02/24/09 16:31:52 (PST)we're on the move again
ODIN NOC: 02/24/09 16:32:04 (PST)I can see ravel getting ready
LRV: 02/24/09 16:33:23 (PST)rascal is in the air. over battle field medic site
ODIN NOC: 02/24/09 16:34:30 (PST)I cannot see it flying on the google earth
LRV: 02/24/09 16:35:12 (PST)maybe a poster issue
ODIN NOC: 02/24/09 16:36:03 (PST)I still see it on the runaway
ODIN Mobile: 02/24/09 16:36:27 (PST)ravens probably over LRV
ODIN NOC: 02/24/09 16:37:03 (PST)is it raven or rascal flying
LRV: 02/24/09 16:37:19 (PST)may have returned, could be raven
LRV: 02/24/09 16:38:20 (PST)correction it was raven not rascal over LRV
ODIN NOC: 02/24/09 16:38:44 (PST)OK
LRV: 02/24/09 16:38:45 (PST)determining if Rascal will fly right now
LRV: 02/24/09 16:39:25 (PST)trying to decide if Rascal needs to fly for ODIN and IPv6 experiments
LRV: 02/24/09 16:41:59 (PST)we have more airtime. can you have tim mcgrew call Dr. B?
ODIN NOC: 02/24/09 16:42:24 (PST)OK
ODIN NOC: 02/24/09 16:43:05 (PST)right now no connection to him but they are on way back to here I think
LRV: 02/24/09 16:43:18 (PST)ok, trying to reach him now
ODIN NOC: 02/24/09 16:43:41 (PST)OK
ODIN Mobile: 02/24/09 16:43:51 (PST)back up

ODIN Mobile: 02/24/09 16:44:17 (PST)tell DR B we're gtg
ODIN Mobile: 02/24/09 16:44:58 (PST)stopped
LRV: 02/24/09 16:45:04 (PST)got it. we have airspace
until 1730. getting rascal ready to fly
LRV: 02/24/09 16:51:30 (PST):-)
ODIN NOC: 02/24/09 16:51:50 (PST)I cannot get your
position for 15 mins
ODIN NOC: 02/24/09 16:52:05 (PST)Is BB working
LRV: 02/24/09 16:54:46 (PST)should soon, rascal is about
to be placed on runway then comms will come up...then BB
posting
ODIN NOC: 02/24/09 16:55:29 (PST)I meant ODIN MOBILE
ODIN Mobile: 02/24/09 16:56:20 (PST)bb battery low
LRV: 02/24/09 16:57:55 (PST)ok, long trip
ODIN NOC: 02/24/09 16:58:00 (PST)I can see you now
ODIN Mobile: 02/24/09 16:57:58 (PST)bb still broadcasting
location
ODIN Mobile: 02/24/09 16:58:12 (PST)on the move again
ODIN Mobile: 02/24/09 16:59:15 (PST)will the rascl remain
over the airfield
LRV: 02/24/09 16:59:47 (PST)rascal taking off
ODIN NOC: 02/24/09 17:00:33 (PST)we lost connection
ODIN NOC: 02/24/09 17:02:39 (PST)Conn back
ODIN NOC: 02/24/09 17:03:58 (PST)Rascal is airborne
ODIN NOC: 02/24/09 17:04:23 (PST)or it's movin on runaway
LRV: 02/24/09 17:07:15 (PST)RASCAL IS OVER lrv
LRV: 02/24/09 17:07:25 (PST)over LRV
ODIN Mobile: 02/24/09 17:08:09 (PST)ask rascal to follow
us
ODIN Mobile: 02/24/09 17:09:15 (PST)plot our location pls
ODIN NOC: 02/24/09 17:10:01 (PST)done
LRV: 02/24/09 17:11:19 (PST)rascal being tasked to take
picture of battlefield medical site
ODIN Mobile: 02/24/09 17:11:55 (PST)roger
ODIN Mobile: 02/24/09 17:12:52 (PST)pls plot location
ODIN Mobile: 02/24/09 17:13:21 (PST)stationary now, take a
measurement of our location and rascal, pls advise of
distance between
ODIN NOC: 02/24/09 17:14:04 (PST)done
ODIN NOC: 02/24/09 17:14:17 (PST)but your BB does not work
for 5 mins
LRV: 02/24/09 17:15:11 (PST)rascal is high over runway rgt
now
ODIN Mobile: 02/24/09 17:15:37 (PST)bb back up
ODIN NOC: 02/24/09 17:16:07 (PST)not yet
LRV: 02/24/09 17:16:10 (PST)rascal on move

ODIN Mobile: 02/24/09 17:16:29 (PST)behind a crest now
with good connectivity
ODIN NOC: 02/24/09 17:17:21 (PST)I cannot see your current
position
ODIN NOC: 02/24/09 17:17:47 (PST)will you pls check BB
again
LRV: 02/24/09 17:18:03 (PST)rascal taking pics over LRV
LRV: 02/24/09 17:18:19 (PST)i read mobile BB pos
ODIN Mobile: 02/24/09 17:18:19 (PST)currently at
10SFE98995950
ODIN NOC: 02/24/09 17:18:51 (PST)ok right now
ODIN Mobile: 02/24/09 17:18:46 (PST)trying to move further
away
ODIN NOC: 02/24/09 17:19:37 (PST)u are 2.5 km far from
Rascal
ODIN NOC: 02/24/09 17:19:45 (PST)Lost conn
ODIN NOC: 02/24/09 17:20:01 (PST)back again
ODIN Mobile: 02/24/09 17:20:28 (PST)moving
ODIN NOC: 02/24/09 17:20:42 (PST)ok
ODIN NOC: 02/24/09 17:20:57 (PST)again no feed from BB
LRV: 02/24/09 17:20:52 (PST)rascal is returning. head
home
ODIN Mobile: 02/24/09 17:21:18 (PST)still receiving data
LRV: 02/24/09 17:21:39 (PST)ok, head back when ready
ODIN NOC: 02/24/09 17:21:49 (PST)4km
ODIN Mobile: 02/24/09 17:21:46 (PST)roger
ODIN Mobile: 02/24/09 17:21:56 (PST)how about now?
ODIN NOC: 02/24/09 17:22:14 (PST)4.5 km from rascal
ODIN NOC: 02/24/09 17:22:29 (PST)5km
ODIN Mobile: 02/24/09 17:22:42 (PST)ok
LRV: 02/24/09 17:22:48 (PST)LRV returning to base
ODIN NOC: 02/24/09 17:22:55 (PST)at home 5.5 km
ODIN Mobile: 02/24/09 17:22:55 (PST)great
ODIN NOC: 02/24/09 17:24:19 (PST)now 5.7 km
ODIN Mobile: 02/24/09 17:24:24 (PST)what was rascals
altitude
ODIN NOC: 02/24/09 17:24:32 (PST)Lost conn to LRV
ODIN NOC: 02/24/09 17:24:50 (PST)I cannot see here
ODIN Mobile: 02/24/09 17:25:03 (PST)pls ask airboss
ODIN NOC: 02/24/09 17:25:16 (PST)nobody here
ODIN NOC: 02/24/09 17:25:28 (PST)I will go out and ask
ODIN Mobile: 02/24/09 17:25:30 (PST)good connectivity when
rascal was airborne
ODIN Mobile: 02/24/09 17:26:05 (PST)on our way back
ODIN_Observer: 02/24/09 17:26:53 (PST)finally

ODIN_Observer: 02/24/09 17:27:25 (PST)does anyone measure the longest distance for connections.

ODIN NOC: 02/24/09 17:32:24 (PST)about 6 km

ODIN NOC: 02/24/09 17:32:55 (PST)altitude was 630 m from ground

C. TF ODIN OBSERVERS NOTE PAD DATA

<i>Date and Time</i>	<i>Comments</i>	<i>Attachment</i>
2/24/2009 5:33:12 PM	Chen: Mobile and Observer will be back.	
2/24/2009 5:31:58 PM	Chen: Mobile and Observer will be back.	
2/24/2009 5:31:26 PM	Chen: The good connection is being maintained when the Rascal is on.	
2/24/2009 5:30:52 PM	Chen: The longest distance for connections is up to 6 km.	
2/24/2009 5:28:39 PM	Chen: The longest distance for connections is up to 6 km.	
2/24/2009 5:18:27 PM	Chen: Tim is recording current vehicle position.	
2/24/2009 5:13:10 PM	Chen: stop and connection is up again.	
2/24/2009 5:08:47 PM	Chen: Stop and check the position of Rascal.	
2/24/2009 5:05:17 PM	ODIN NOC: Conn back again	
2/24/2009 5:05:01 PM	ODIN NOC: Lost Connection	
2/24/2009 5:00:48 PM	ODIN NOC: Lost conn again	
2/24/2009 4:56:58 PM	Chen: Stop again and connection is on.	
2/24/2009 4:55:48 PM	ODIN NOC: Connection up again	
2/24/2009 4:53:47 PM	Chen: wait for rascal.	
2/24/2009 4:53:01 PM	ODIN NOC: Lost Connection	Replace Delete
2/24/2009 4:51:33 PM	Chen: Move Back.	

2/24/2009 4:45:52 PM	ODIN NOC: Connection back	
2/24/2009 4:43:22 PM	ODIN NOC: Lost Connection	
2/24/2009 4:42:23 PM	LRV_NOC: Tim call Dr B if available	
2/24/2009 4:39:27 PM	ODIN NOC: Conn back	Replace Delete
2/24/2009 4:37:53 PM	ODIN NOC: Lost connection	Replace Delete
2/24/2009 4:37:02 PM	Chen: Move Back.	
2/24/2009 4:36:22 PM	ODIN NOC: ODIN_4 is back	
2/24/2009 4:35:20 PM	ODIN NOC: Lost conn with ODIN_4	
2/24/2009 4:33:41 PM	LRV_NOC: rascal airborne over LRV	
2/24/2009 4:21:40 PM	Chen: 1620 we`ll get back to NOC.	
2/24/2009 4:19:01 PM	ODIN NOC: It`s UP	
2/24/2009 4:18:28 PM	ODIN NOC: Lost conn again	
2/24/2009 4:17:50 PM	ODIN NOC: Things are good	
2/24/2009 4:16:45 PM	ODIN NOC: We have problem with connection then it`s up again	
2/24/2009 4:13:39 PM	Chen: 1611 The connection is up again and we keep moving on.	
2/24/2009 4:12:46 PM	ODIN NOC: We still have connection	Replace Delete
2/24/2009 4:07:47 PM	LRV_NOC: situational awareness note: injured person. network nodes should optimize for battlefield medical evac...test, test, test	
2/24/2009 4:05:03 PM	Chen: 1602 We stop at the position 10SGE0042 5575 and the connections are still on.	
2/24/2009 4:01:26 PM	Chen: 1601 The vehicle is moving on again.	
2/24/2009 4:00:40 PM	Chen: 1600 Raven will be launched again.	

2/24/2009 4:00:29 PM	ODIN NOC: 35 43 09.41N 120 46 26.89W	Replace Delete
2/24/2009 3:59:05 PM	Chen: 1552 We lost connections and backup in 1 minute.	
2/24/2009 3:58:07 PM	ODIN NOC: Nodes are up again	
2/24/2009 3:55:26 PM	ODIN NOC: We lost connection	Replace Delete
2/24/2009 3:55:01 PM	LRV_NOC: maybe shift to just chat...less bandwidth	
2/24/2009 3:53:44 PM	ODIN NOC: We could hardly talk on VC1	
2/24/2009 3:49:35 PM	Chen: 1540 We conduct communications with VC1 based on wave-realy at position 10N701293 3959079.	
2/24/2009 3:48:20 PM	Chen: 1536 The Vehicle is moving on for the wave-relay experiment.	
2/24/2009 3:45:15 PM	Chen: 1535 Raven landed.	
2/24/2009 3:40:52 PM	ODIN NOC: No connection at the beginning	
2/24/2009 3:39:56 PM	ODIN NOC: Team departed	Replace Delete
2/24/2009 3:30:45 PM	LRV_NOC: how are comms now?	
2/24/2009 3:18:11 PM	ODIN NOC: We lost connection time to time	Replace Delete
2/24/2009 3:18:07 PM	LRV_NOC: any one on the net?	
2/24/2009 3:15:19 PM	LRV_NOC: this is LRV with test comms check	
2/24/2009 3:08:39 PM	Chen: 1505 The Second Time, Raven took off.	
2/24/2009 2:50:24 PM	Chen: 1444 Raven took off.	
2/24/2009 1:57:01 PM	Chen: 1310~1330 Kristine in NPS and Chen in vehicle tested communications by voice, message, chat, and file sharing with Groove and VC1. It works well also. The testing for MIO project is done today.	
2/24/2009 1:15:00 PM	Chen: 1250~1310 Tim, Mustafa, and Chen set up laptops, radios, and a camera and tested connections in	

	order for experiments.	
2/24/2009 12:47:22 PM	Chen: 1215~1245 Mustafa, Chen, and Kristine in NPS conduct CT experiments for the MIO project via Groove and VC1 application. We tested Chat, Voice, File Sharing, and Video communication during experiments. It works well.	Replace Delete
2/24/2009 12:00:59 PM	Chen: 1155 Mustafa and Chen finished testing communication via MS Groove. Later, we`ll conduct experiments with Kristine in NPS for the collaborative technology project.	
2/24/2009 11:54:02 AM	Chen: 1120~1150 Mustafa is adding nodes to the network via SolarWinds.	
2/24/2009 10:50:42 AM	Chen: 1000~1030 network connection configuration, SolarWinds test, and VC1 Test for ODIN experiments.	

***[Replace_Delete](#) indicates an attached file**

D. PARAFOIL SIGNIFICANT EVENTS RECORD

2/24/2009 1:17:53 PM	CR_NOC: SF2 on ground
2/24/2009 1:15:29 PM	CR_NOC: SF1 in on ground, missed target. SF2 accepted new target
2/24/2009 1:14:45 PM	CR_NOC: SF2 retasked
2/24/2009 1:14:00 PM	CR_NOC: SF1 retaksed
2/24/2009 1:13:10 PM	CR_NOC: snowflake 2 dropped target, reset to default
2/24/2009 1:12:40 PM	CR_NOC: snowflake 1 dropped target, snowflake 2 tasked with target
2/24/2009 1:12:03 PM	CR_NOC: snowflake 2 dropped
2/24/2009 1:11:50 PM	CR_NOC: 30 secs until drop 2
2/24/2009 1:11:37 PM	CR_NOC: snowflake 1 is intermittent on accepting target data
2/24/2009 1:10:25 PM	CR_NOC: snowflake 1 not taking user ID 25. resetting to default drop point

2/24/2009 1:09:23 PM	CR_NOC: snowflake 1 tasked
2/24/2009 1:08:44 PM	CR_NOC: snowflake 1 dropped
2/24/2009 1:03:10 PM	CR_NOC: cesna airborne, climbing to 5000 ft for 2nd pass. 1st pass was made at 3500 ft.
2/24/2009 1:02:27 PM	CR_NOC: cesna taking off for 2nd pass
2/24/2009 12:17:45 PM	CR_NOC: cessna on ground
2/24/2009 12:10:19 PM	CR_NOC: parafoil recovery beginning
2/24/2009 12:08:05 PM	CR_NOC: snowflake 2 missed target by 90 meters
2/24/2009 12:07:51 PM	CR_NOC: snowflake targets received target data, but not sender ID.
2/24/2009 12:05:47 PM	CR_NOC: snowflake #1 missed target. snowflake #2 is currently on course
2/24/2009 12:03:46 PM	CR_NOC: target is assigned snowflake 2
2/24/2009 12:03:07 PM	CR_NOC: parafoil #2 is dropped
2/24/2009 12:00:36 PM	CR_NOC: target is assigned 23-25 snowflake 1
2/24/2009 11:59:44 AM	CR_NOC: parafoil is dropped
2/24/2009 11:57:58 AM	CR_NOC: parafoil to drop in 60 secs
2/24/2009 11:53:55 AM	CR_NOC: Cessna is airborne
2/24/2009 11:50:49 AM	CR_NOC: Cessna is taking off
2/24/2009 11:37:18 AM	CR_NOC: This is start of Parafoil Experiment

E. REMOTE MONITORING OF REDLINE RADIO AN-80I CHAT LOG

TOC: 02/25/09 13:04:32 (PST)test toc

LRV: 02/25/09 14:10:41 (PST)look for 192.168.99.35 and 36

LRV: 02/25/09 14:15:19 (PST)i can see .36 and .35 in solarwinds discovery

Bob: 02/25/09 14:16:44 (PST)testing

Ryan: 02/25/09 14:16:53 (PST>Hello

Ryan: 02/25/09 14:19:53 (PST)Bob can ping the 80i but is having a hard time finding it in dopplervue

LRV: 02/25/09 14:20:15 (PST)make sure to rerun the discovery

LRV: 02/25/09 14:21:03 (PST)you can try and discover just .35 and .36

Ryan: 02/25/09 14:21:09 (PST)he did an individual discovery but can't get any traffic coming from it

Ryan: 02/25/09 14:21:14 (PST)he did that

LRV: 02/25/09 14:21:35 (PST)hmmmm

Ryan: 02/25/09 14:23:24 (PST)individual device discovery - add it as a link, a node, a workstation?

LRV: 02/25/09 14:24:52 (PST)i have uploaded a screen capture of the 80i MIB from SW Eng tool set in File repository

LRV: 02/25/09 14:25:19 (PST)maybe add as a link or node?

Bob: 02/25/09 14:27:45 (PST)running discovery at this time

Bob: 02/25/09 14:27:53 (PST)tango down!!! tango down!!!

Bob: 02/25/09 14:30:31 (PST)192.168.98.71

LRV: 02/25/09 14:30:33 (PST)both of you may not have snmp enabled and firewalls blocking pings

Bob: 02/25/09 14:30:34 (PST)try .72

Ryan: 02/25/09 14:30:41 (PST)Bravo Whiskey!

Bob: 02/25/09 14:30:53 (PST)CHARLIE FOXTROT!!!

LRV: 02/25/09 14:45:19 (PST)LRV starting to Tear down. checking out

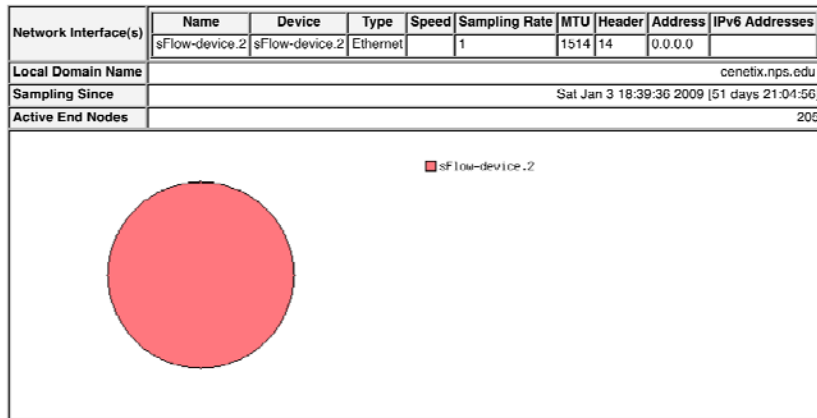
APPENDIX B: SFLOW SCREEN CAPTURES



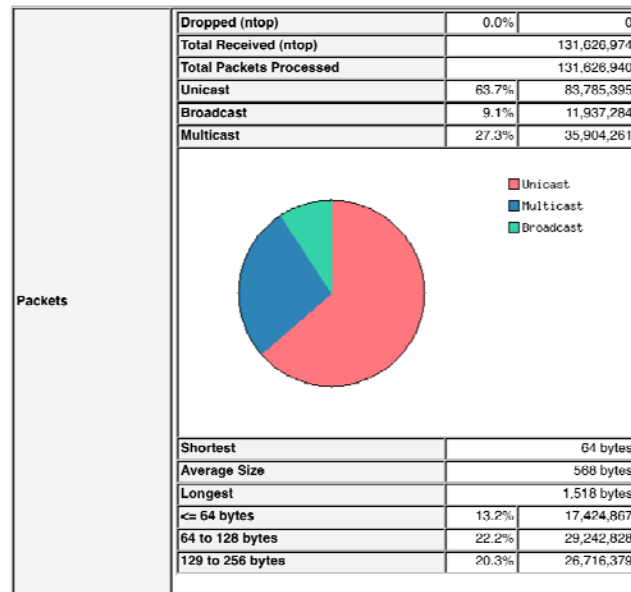
About Summary All Protocols IP Media Utils Plugins Admin

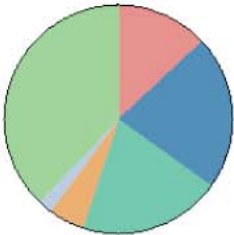
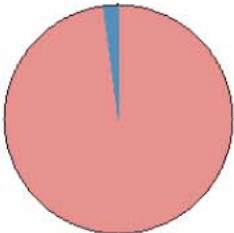
(C) 1998-2005 - Luca Deri

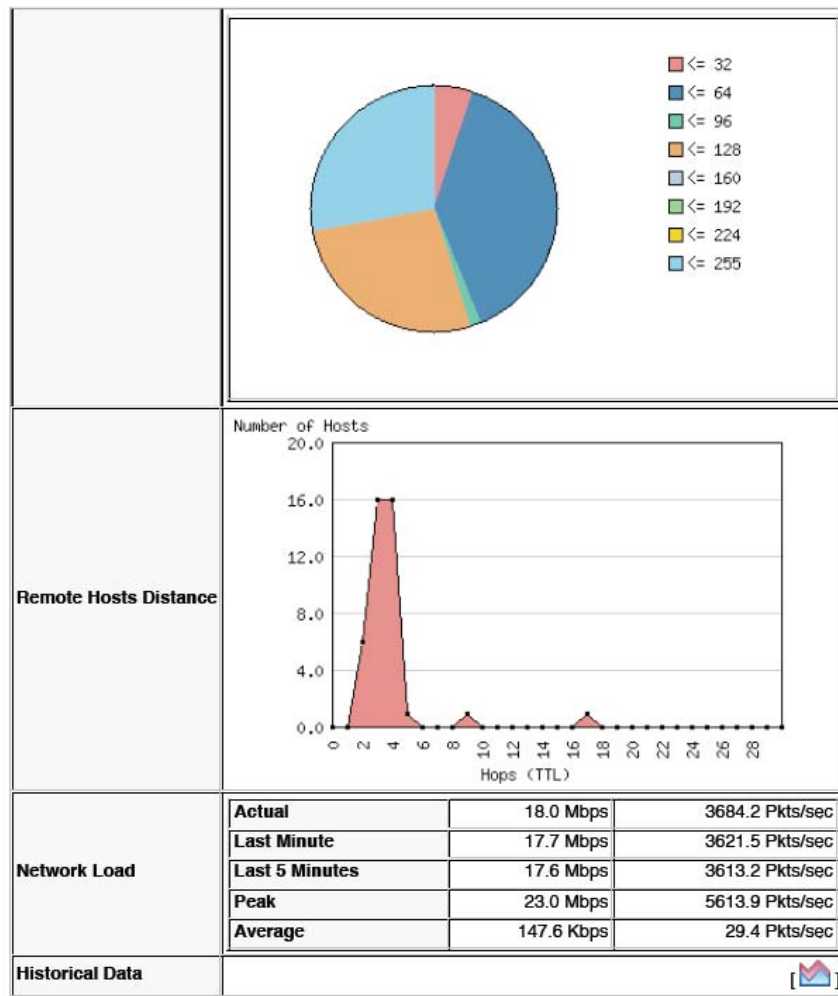
Global Traffic Statistics



Traffic Report for 'sFlow-device.2' [switch]

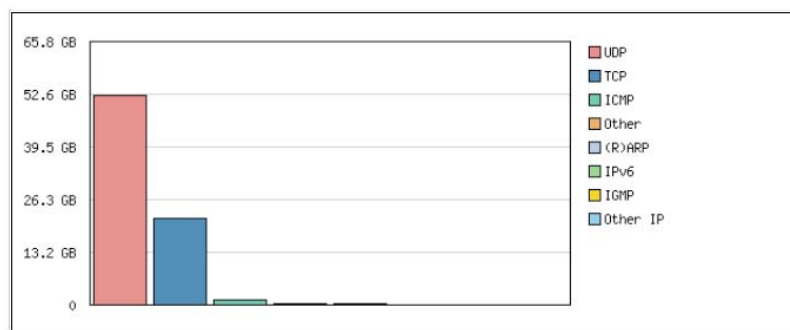


	257 to 512 bytes		5.0%	6,613,569
	513 to 1024 bytes		2.0%	2,644,635
	1025 to 1518 bytes		37.2%	48,984,662
	> 1518 bytes		0.0%	0
				
	Packets too long (> 1514)		9.1%	11,992,950
	Bad Packets (Checksum)		0.0%	0
Traffic	Total		77.0 GB [131,626,940 Pkts]	
	IP Traffic		75.9 GB [75.9 GB Pkts]	
	Fragmented IP Traffic		27.5 MB [0.0%]	
	Non IP Traffic		1.1 GB	
				
	Average TTL		116	
	TTL <= 32		5.0%	6,578,887
	32 < TTL <= 64		35.6%	46,891,661
	64 < TTL <= 96		1.3%	1,721,572
	96 < TTL <= 128		24.8%	32,621,496
	128 < TTL <= 160		0.0%	30
	160 < TTL <= 192		0.0%	29
	192 < TTL <= 224		0.0%	26
	224 < TTL <= 256		25.5%	33,531,983



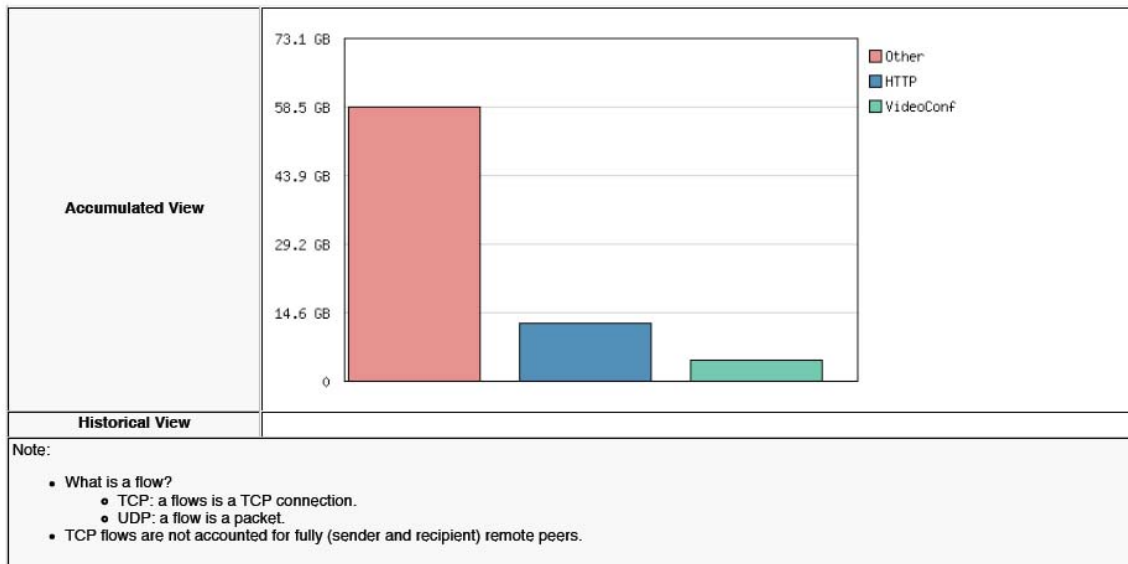
Global Protocol Distribution

Protocol	Data	Percentage				
IP	75.9 GB	98.5%	TCP	21.8 GB	28.7%	<div></div>
			UDP	52.7 GB	69.4%	<div></div>
			ICMP	1.4 GB	1.8%	<div></div>
			ICMPv6	41.5 MB	0%	
			IGMP	5.5 MB	0%	
			Other IP	2.3 MB	0%	
(R)ARP	362.6 MB	0%				
IPv6	52.6 MB	0%				
Other	563.0 MB	0%				



Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Flows	Accumulated Percentage / Historical Protocol View	
SA	125.2 MB	32	0%	<p>Bytes/sec</p> <p>Min: 0.0 Max: 129.7k Avg: 3.0k Current: 7.8k</p>
CoT	138.0 MB	358,320	0%	
VideoCont	4.7 GB	1,975	6.2%	
HTTP	12.6 GB	30,752	16.6%	
FTP	3.4 MB	10	0%	
DNS	10.6 MB	109,501	0%	
SNMP	719.7 MB	8,190,327	0%	
Telnet	35.8 KB	4	0%	
NetBIOS	556.7 MB	1,991,399	0%	
NetFlow	1.3 MB	13,704	0%	
Other TCP/UDP-based Protocols	57.1 GB	71,145,096	75.2%	



TCP/UDP Traffic Port Distribution: Last Minute View

TCP/UDP Port		Total	Sent	Recv
boinc-client	1043	44.1 GB	44.1 GB	105.6 KB
sflow	6343	44.1 GB	0	44.1 GB
http	80	12.6 GB	12.2 GB	370.4 MB
tivoli-npm	1965	11.2 GB	239.6 MB	11.0 GB
macromedia-ics	1935	4.8 GB	3.0 GB	1.8 GB
microsoft-ds	445	3.9 GB	123.2 MB	3.8 GB
mstw-s-storage	2172	3.8 GB	3.7 GB	58.3 MB
11002	11002	1.5 GB	0	1.5 GB
11004	11004	1.4 GB	0	1.4 GB
11006	11006	1.2 GB	0	1.2 GB
elvin_client	2917	882.9 MB	882.7 MB	230.5 KB
55000	55000	882.4 MB	2.4 KB	882.4 MB
6420	6420	757.1 MB	757.1 MB	0
39090	39090	723.8 MB	0	723.8 MB
snmp	161	719.7 MB	257.0 MB	462.7 MB
6419	6419	677.8 MB	0	677.8 MB
ea1	1791	645.8 MB	235.4 MB	410.3 MB
39080	39080	642.5 MB	544	642.5 MB
tns-adv	3309	628.6 MB	437.6 MB	191.1 MB
4082	4082	598.7 MB	390.1 MB	208.6 MB
52854	52854	565.0 MB	565.0 MB	1.9 KB
42528	42528	561.8 MB	561.8 MB	0
ctp	3772	506.3 MB	15.6 MB	490.7 MB
37466	37466	497.4 MB	497.4 MB	0
49271	49271	496.6 MB	194.8 MB	301.7 MB
checksum	1386	433.4 MB	106.4 MB	327.1 MB
netbios-ssn	139	353.0 MB	79.1 MB	273.9 MB
netbios-ns	137	347.4 MB	173.7 MB	173.7 MB
49509	49509	324.2 MB	116.4 MB	207.7 MB

novell-lu6.2	1416	286.7 MB	207.1 MB	79.6 MB
1138	1138	263.3 MB	12.3 MB	251.1 MB
45879	45879	253.9 MB	253.9 MB	0
Notes: <ul style="list-style-type: none"> • sum(total traffic per port) = 2*(total IP traffic) because the traffic per port is counted twice (sent and received) • This report includes broadcast packets 				

This extract is just a sample of the packets ntop has seen.

Report created on Tue Feb 24 15:44:32 2009 [ntop uptime: 51 days 21:04:56]
Generated by ntop v.3.2 (Dag Apt RPM Repository) [i686-redhat-linux-gnu]
© 1998-2005 by Luca Deri, built: Apr 29 2006 19:31:55.
Listening on [sFlow-device.2] for all packets (i.e. without a filtering expression)
Web reports include only interface "sFlow-device.2"

LIST OF REFERENCES

- [1] S. Keshav and R. Sharma, "Achieving Quality of Service through Network Performance Management," presented at the 8th International Workshop on Network and Operating Systems Support for Digital Audio and Video, Cambridge, England, 1998.
- [2] A. K. Cebrowski, VAdm, USN and J. J. Garstka, "Network Centric Warfare: Its Origin and Future." Proceedings of the Naval Institute, vol. 124:1, 1998, pp 28-35.
- [3] Department of Defense, "Joint Publication 13: Information Operations," 2006, p I-5.
- [4] D. S. Alberts, J. J Garstka and F. P. Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority". Washington DC: CCRP Publication Series, 1999, pp 88-94.
- [5] A. K. Cebrowski, VAdm, USN and J. J. Garstka, "Network Centric Warfare: Its Origin and Future." Proceedings of the Naval Institute, vol. 124:1, 1998, pp 28-35
- [6] D. S. Alberts, J. J Garstka and F. P. Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority." Washington DC: Command and Control Research Program Publication Series, 1999, pp 187-192.
- [7] "Network Centric Warfare Conceptual Framework," introductory brief for Network Centric Warfare and Network Enabled Capabilities Workshop, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OSD/NII) in conjunction with RAND and Effects Based Research, Inc (ERB), December 2002
http://www.dodccrp.org/events/2002_ncw_workshop/NCWDecWork.htm, February 2009.
- [8] Department of Defense Chief Information Officer, "Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service Oriented DoD Enterprise," Version 1.0, 2007,

- [9] R. Schollmeier, "A Definition of *Peer-to-Peer* Networking for the Classification of *Peer-to-Peer* Architectures and Applications," in *Proceedings of the First International Conference on Peer-to-Peer Computing (P2P'01)*, 2002.
- [10] J. Lu and J. Callan, "Content-Based Retrieval in Hybrid Peer-to-Peer Networks," in *International Conference on Information Knowledge Management*, 2003.
- [11] International Standards Organization, "*ISO/IEC 7498-4: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management Framework*," 1989.
- [12] L. Lewis, "Managing Computer Networks: Case-Based Reasoning Approach," Boston: Artech House, Inc., 1995, pp 3-12.
- [13] M. Subramanian, "Network Management: Principles and Practice," Boston: Addison Wesley, 2006, pp. 40-45.
- [14] P. Senge, "The Fifth Discipline: The Art & Practice of the Learning Organization," New York: Currency DoubleDay, 1990, p. 14.
- [15] Department of Defense Command and Control Research Program, "Enabling Effective Collaboration in Military Operations," presentations from Enabling Effective in Military Operations Workshop, Vienna, Virginia, 2001.
- [16] J. Glass, "Taking Aim in Afghanistan: Army anti-IED task force to take on the Taliban, al-Qaida," C4ISR Journal: The Magazine of Net-Centric Warfare, February 2009, <http://www.c4isrjournal.com/story.php?F=3825704>, February 2009.
- [17] A. Ball and B. McCutchen Jr. "Task Force ODIN Using Innovative Technology to Support Ground Forces," Digital Video and Imagery Distribution System, September 2007, http://dvidshub.net/?script=news/news_show.php&id=12463, February 2009.

- [18] K. Osborn, "Army sends ODIN to Afghanistan," Army Times, December 2008,
http://www.armytimes.com/news/2008/12/web_defense_121508_army_ODIN/, January 2009.
- [19] J. Postel, "RFC792 - Internet Control Messaging Protocol," ISI, 1981,
<http://www.faqs.org/rfcs/rfc792.html>, February 2009.
- [20] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "RFC1157 - Simple Network Management Protocol (SNMP)," SNMP Research, 1990,
<http://www.faqs.org/rfcs/rfc1157.html>, February 2009.
- [21] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "RFC1901 - Introduction to Community-based SNMPv2," SNMPv2 Working Group, 1996,
<http://www.faqs.org/rfcs/rfc1901.html>, February 2009.
- [22] M. Subramanian, "Network Management: Principles and Practice," Boston: Addison Wesley, 2006, pp. 141-282.
- [23] A. Bordetsky and R. Hayes-Roth, "Extending the OSI Model for Wireless Battlefield Networks: A Design Approach to the 8th Layer for Tactical Hyper-nodes," International Journal of Mobile Network Design and Innovation, vol. 2: issue 2, 2007, pp. 81-91.
- [24] Cisco, "NetFlow Services Solution Guide," May 2001,
http://www.cisco.com/en/US/products/sw/netmgts/ps1964/products_implementation_design_guide09186a00800d6a11.html#wp1030045, February 2009.
- [25] InMon Corporation, "sFlow," 2009,
<http://www.inmon.com/technology/index.php>, February 2009.
- [26] E.Jasinska, "sFlow Datagram," 2006, Amsterdam Internet Exchange (AMS-IX B.V.),
<http://www.sflow.org/developers/specifications.php>, February 2009.
- [27] sFlow.org, "Traffic Monitoring using sFlow®," 2003,
<http://www.sflow.org/sFlowOverview.pdf>, February 2009.

- [28] IP Information Flow Export Working Group, "Charter," December 2008,
<http://www.ietf.org/html.charters/ipfix-charter.html>,
February 2009.
- [29] M. Klein, D. Plakosh, and K. Wallnau, "An Auction Mechanism for Allocating Bandwidth for Data Fusion in Tactical Data Networks: A Close Study of Computational Mechanism Design," January 2008, Carnegie Mellon University, Pittsburgh, PA.
- [30] A. Bordetsky and M. Clement, "Cursor on-Target Message Networks for Unmanned Aerial Vehicles," Naval Postgraduate School, Monterey, CA, 2009
- [31] Boeing, "Boeing, U.S. Air Force Demonstrate Advanced Airborne Networking First," January 2007,
http://www.boeing.com/news/releases/2007/q1/070116b_nr.html, February 2009.
- [32] Information Processing Techniques Office, Defense Advanced Research Projects Agency (DARPA), "Situation Aware Protocols in Edge Networking Technologies Mission Statement," August 2004,
<http://www.darpa.mil/ipto/programs/sapient/sapient.asp>
February 2009.
- [33] Information Processing Techniques Office, Defense Advanced Research Projects Agency (DARPA), "BAA 04-32 PROPOSER INFORMATION PAMPHLET," August 2004,
<http://www.darpa.mil/ipto/programs/sapient/sapient.asp>
February 2009.
- [34] P. Lardieri and D. Dacosta, "Synthesizing Adaptive Protocols by Selective Enumeration (SYNAPSE): BAA 04-32 Situation Aware Protocols in Edge Network Technologies (SAPIENT)," Lockheed Martin Advanced Technology Laboratories, Drexel University, 2008.
- [35] A Bordetsky and D. Netzer, "TNT Experimentation Campaign and Testbed," Presentation for the U.S. Special Operations Command - Naval Postgraduate School Cooperative, Naval Postgraduate School at Monterey, California, Fall 2008.

- [36] S. Rolle, "Measures of Progress for Collaboration: Case Study for the Applegate Partnership," U.S. Department of Agriculture, Pacific Northwest Research Station, Portland, Oregon, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Dr. Alex Bordetsky
Naval Postgraduate School
Monterey, California
4. Lt Col Karl Pfeiffer
Naval Postgraduate School
Monterey, California
5. Dr. Raymond Buettner
Naval Postgraduate School
Monterey, California
6. Michael Deacy
U.S. Special Operations Command
Tampa, Florida